

501P1180300 4

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 7月24日

出 願 番 号

Application Number:

特願2000-222125

出 願 人

Applicant(s):

ソニー株式会社

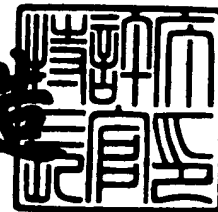
11050 U.S. PTO
09/911886
07/24/01

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 5月11日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3038642

【書類名】 特許願

【整理番号】 00006009

【提出日】 平成12年 7月24日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 19/00

【発明の名称】 データ処理装置およびデータ処理方法、並びにプログラム提供媒体

【請求項の数】 15

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 岡上 拓己

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100101801

 【弁理士】

 【氏名又は名称】 山田 英治

 【電話番号】 03-5541-7577

【選任した代理人】

 【識別番号】 100093241

 【弁理士】

 【氏名又は名称】 宮田 正昭

 【電話番号】 03-5541-7577

【選任した代理人】

 【識別番号】 100086531

 【弁理士】

【氏名又は名称】 澤田 俊夫

【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 062721

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ処理装置およびデータ処理方法、並びにプログラム提供媒体

【特許請求の範囲】

【請求項 1】

記憶装置に格納されるコンテンツの検証値を生成してコンテンツに対応付けて格納し、コンテンツ改竄の有無を前記検証値により実行するデータ処理装置であり、

前記検証値は、コンテンツのカテゴリ毎に独立した検証値として生成して格納する構成を有することを特徴とするデータ処理装置。

【請求項 2】

前記データ処理装置は、

コンテンツ利用に際して、利用対象コンテンツ構成データに基づいて検証値を算出し、該算出検証値と、予め格納された検証値との比較処理を実行し、一致する場合にのみコンテンツ利用を可能とした構成を有することを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 3】

前記記憶装置は、複数のディレクトリの各々に異なるカテゴリのコンテンツデータを格納する構成を有し、

前記検証値は、前記複数のディレクトリの各々を単位とするコンテンツの集合に対して生成される値であることを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 4】

前記記憶装置は、フラッシュメモリであり、

前記カテゴリ毎の検証値は、フラッシュメモリの使用禁止ブロックとして設定された領域に格納される構成を有することを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 5】

前記カテゴリは、コンテンツの種類に基づいて設定された構成であり、

コンテンツの種類別に独立した検証値を設定し、格納する構成を有することを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 6】

前記カテゴリは、コンテンツの暗号処理鍵として設定されるコンテンツキー K c o n を暗号化して提供する有効化キーブロック (E K B) の管理エンティティに基づいて設定された構成であり、

有効化キーブロック (E K B) の管理エンティティ別に独立した検証値を設定し、格納する構成を有することを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 7】

前記検証値は、検証対象となるコンテンツおよびヘッダ情報等のコンテンツ関連データを構成する部分データをメッセージとして D E S 暗号処理によって生成されるメッセージ認証符号 (M A C) に基づいて生成されるデータであることを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 8】

記憶装置に格納されるコンテンツの検証値を生成してコンテンツに対応付けて格納し、コンテンツ改竄の有無を前記検証値により実行するデータ処理方法であり、

前記検証値を、コンテンツのカテゴリ毎に独立した検証値として生成して格納することを特徴とするデータ処理方法。

【請求項 9】

前記データ処理方法において、さらに、

コンテンツ利用に際して、利用対象コンテンツ構成データに基づいて検証値を算出し、該算出検証値と、予め格納された検証値との比較処理を実行し、一致する場合にのみコンテンツ利用を行なうことを特徴とする請求項 8 に記載のデータ処理方法。

【請求項 1 0】

前記記憶装置は、複数のディレクトリの各々に異なるカテゴリのコンテンツデータを格納する構成を有し、

前記検証値は、前記複数のディレクトリの各々を単位とするコンテンツの集合

に対して生成することを特徴とする請求項 8 に記載のデータ処理方法。

【請求項 1 1】

前記記憶装置は、フラッシュメモリであり、

前記カテゴリ毎の検証値は、フラッシュメモリの使用禁止ブロックとして設定された領域に格納することを特徴とする請求項 8 に記載のデータ処理方法。

【請求項 1 2】

前記カテゴリは、コンテンツの種類に基づいて設定され、

コンテンツの種類別に独立した検証値を設定し、格納することを特徴とする請求項 8 に記載のデータ処理方法。

【請求項 1 3】

前記カテゴリは、コンテンツの暗号処理鍵として設定されるコンテンツキー K c o n を暗号化して提供する有効化キーブロック (E K B) の管理エンティティに基づいて設定され、

有効化キーブロック (E K B) の管理エンティティ別に独立した検証値を設定し、格納することを特徴とする請求項 8 に記載のデータ処理方法。

【請求項 1 4】

前記検証値は、検証対象となるコンテンツおよびヘッダ情報等のコンテンツ関連データを構成する部分データをメッセージとして D E S 暗号処理によって生成されるメッセージ認証符号 (M A C) に基づいて生成されるデータであることを特徴とする請求項 8 に記載のデータ処理方法。

【請求項 1 5】

記憶装置に格納されるコンテンツの検証値を生成してコンテンツに対応付けて格納し、コンテンツ改竄の有無を前記検証値により実行するデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

検証値を、コンテンツのカテゴリ毎に独立した検証値として生成して格納するステップを有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【 0 0 0 1】

【発明の属する技術分野】

本発明は、データ処理装置およびデータ処理方法、並びにプログラム提供媒体に関する。特に、記憶装置に格納されるコンテンツの検証値を生成してコンテンツに対応付けて格納し、コンテンツ改竄の有無を前記検証値により実行する構成において、検証値をコンテンツのカテゴリ毎に独立した検証値として生成して格納する構成とし、コンテンツ改竄チェック処理の効率化を実現したデータ処理装置およびデータ処理方法、並びにプログラム提供媒体に関する。

【0002】

【従来の技術】

昨今、音楽データ、ゲームプログラム、画像データ等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット等のネットワーク、あるいは、メモリカード、DVD、CD等の流通可能な記憶媒体を介して流通させるコンテンツ流通が盛んになってきている。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、再生専用器、あるいはゲーム機器におけるコンテンツデータの受信、あるいはメモリカード、CD、DVD等の記憶媒体の装着により、コンテンツ再生処理が実行されたり、あるいは外部からの入力コンテンツを再生器、PC等に内蔵の記録デバイス、例えばメモリカード、ハードディスク等に格納し、再度、格納媒体から再生する等の方法により利用される。

【0003】

再生装置、ゲーム機器、PC等の情報機器には、流通コンテンツをネットワークから受信するため、あるいはDVD、CD等にアクセスするためのインタフェースを有し、さらにコンテンツの再生に必要な制御手段、プログラム、データのメモリ領域として使用されるRAM、ROM等を有する。

【0004】

音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生機器として利用される再生装置、ゲーム機器、PC等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により、例えば内蔵、あるいは着脱自在の記憶媒体から呼び出され、情報機器本体、あるいは接続さ

れたディスプレイ、スピーカ等を通じて再生される。

【 0 0 0 5 】

ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないうにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【 0 0 0 6 】

ユーザに対する利用制限を実現する 1 つの手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

【 0 0 0 7 】

暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【 0 0 0 8 】

暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その 1 つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式に D E S（データ暗号標準：Data encryption standard）がある。

【 0 0 0 9 】

上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパ

スワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【 0 0 1 0 】

また、暗号化するとき使用する暗号化鍵による処理と、復号するとき使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものには R S A (Rivest-Shamir-Adleman) 暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

【 0 0 1 1 】

【発明が解決しようとする課題】

コンテンツデータの正当性、すなわちデータが改竄されていないことをチェックするために検証用のチェック値を正規のコンテンツデータに基づいて生成して予めメモリに格納し、コンテンツ利用時に検証対象のデータに基づいて生成したチェック値と格納チェック値とを照合処理することによって、データ検証を行なう方法が従来から行なわれている。

【 0 0 1 2 】

しかしながら、メモリに格納するコンテンツ数が増大すると、検証用のチェック値を正規のコンテンツデータに基づいて生成し、格納し管理することが困難となる。特に、昨今フラッシュメモリを使用したメモリカード等の容量の大きい媒

体においては、音楽データ、画像データ、プログラムデータ等、様々なカテゴリのコンテンツデータがメモリに格納されることとなる。このような環境においては、コンテンツのチェック値の生成処理、格納処理、改竄チェック処理の管理は困難となる。格納データ全体に対するチェック値を生成すると、チェック対象となったデータ全体に対するチェック値生成処理を実行することが必要となる。例えばDES-CBCモードにおいて生成されるメッセージ認証符号（MAC）により、チェック値ICVを求める手法を行なう場合、データ全体に対するDES-CBCの処理を実行することが必要となる。この計算量は、データ長が長くなるにつれ増大することとなり、処理効率の点で問題がある。

【0013】

本発明は、このような従来技術の問題点を解決するものであり、データ正当性の確認処理を効率的に実行し、コンテンツデータの検証処理の効率化、さらに検証後の記録デバイスに対するダウンロード処理、あるいは検証後の再生処理等を効率的に実行することを可能とするデータ処理装置およびデータ処理方法、並びにプログラム提供媒体を提供することを目的とする。

【0014】

【課題を解決するための手段】

本発明の第1の側面は、

記憶装置に格納されるコンテンツの検証値を生成してコンテンツに対応付けて格納し、コンテンツ改竄の有無を前記検証値により実行するデータ処理装置であり、

前記検証値は、コンテンツのカテゴリ毎に独立した検証値として生成して格納する構成を有することを特徴とするデータ処理装置にある。

【0015】

さらに、本発明のデータ処理装置の一実施態様において、前記データ処理装置は、コンテンツ利用に際して、利用対象コンテンツ構成データに基づいて検証値を算出し、該算出検証値と、予め格納された検証値との比較処理を実行し、一致する場合にのみコンテンツ利用を可能とした構成を有することを特徴とする。

【0016】

さらに、本発明のデータ処理装置の一実施態様において、前記記憶装置は、複数のディレクトリの各々に異なるカテゴリのコンテンツデータを格納する構成を有し、前記検証値は、前記複数のディレクトリの各々を単位とするコンテンツの集合に対して生成される値であることを特徴とする。

【 0 0 1 7 】

さらに、本発明のデータ処理装置の一実施態様において、前記記憶装置は、フラッシュメモリであり、前記カテゴリ毎の検証値は、フラッシュメモリの使用禁止ブロックとして設定された領域に格納される構成を有することを特徴とする。

【 0 0 1 8 】

さらに、本発明のデータ処理装置の一実施態様において、前記カテゴリは、コンテンツの種類に基づいて設定された構成であり、コンテンツの種類別に独立した検証値を設定し、格納する構成を有することを特徴とする。

【 0 0 1 9 】

さらに、本発明のデータ処理装置の一実施態様において、前記カテゴリは、コンテンツの暗号処理鍵として設定されるコンテンツキー *Kcon* を暗号化して提供する有効化キーブロック (EKB) の管理エンティティに基づいて設定された構成であり、有効化キーブロック (EKB) の管理エンティティ別に独立した検証値を設定し、格納する構成を有することを特徴とする。

【 0 0 2 0 】

さらに、本発明のデータ処理装置の一実施態様において、前記検証値は、検証対象となるコンテンツおよびヘッダ情報等のコンテンツ関連データを構成する部分データをメッセージとして DES 暗号処理によって生成されるメッセージ認証符号 (MAC) に基づいて生成されるデータであることを特徴とする。

【 0 0 2 1 】

さらに、本発明の第 2 の側面は、

記憶装置に格納されるコンテンツの検証値を生成してコンテンツに対応付けて格納し、コンテンツ改竄の有無を前記検証値により実行するデータ処理方法であり、

前記検証値を、コンテンツのカテゴリ毎に独立した検証値として生成して格納

することを特徴とするデータ処理方法にある。

【 0 0 2 2 】

さらに、本発明のデータ処理方法の一実施態様において、コンテンツ利用に際して、利用対象コンテンツ構成データに基づいて検証値を算出し、該算出検証値と、予め格納された検証値との比較処理を実行し、一致する場合にのみコンテンツ利用を行なうことを特徴とする。

【 0 0 2 3 】

さらに、本発明のデータ処理方法の一実施態様において、前記記憶装置は、複数のディレクトリの各々に異なるカテゴリのコンテンツデータを格納する構成を有し、前記検証値は、前記複数のディレクトリの各々を単位とするコンテンツの集合に対して生成することを特徴とする。

【 0 0 2 4 】

さらに、本発明のデータ処理方法の一実施態様において、前記記憶装置は、フラッシュメモリであり、前記カテゴリ毎の検証値は、フラッシュメモリの使用禁止ブロックとして設定された領域に格納することを特徴とする。

【 0 0 2 5 】

さらに、本発明のデータ処理方法の一実施態様において、前記カテゴリは、コンテンツの種類に基づいて設定され、コンテンツの種類別に独立した検証値を設定し、格納することを特徴とする。

【 0 0 2 6 】

さらに、本発明のデータ処理方法の一実施態様において、前記カテゴリは、コンテンツの暗号処理鍵として設定されるコンテンツキー K c o n を暗号化して提供する有効化キーブロック (E K B) の管理エンティティに基づいて設定され、有効化キーブロック (E K B) の管理エンティティ別に独立した検証値を設定し、格納することを特徴とする。

【 0 0 2 7 】

さらに、本発明のデータ処理方法の一実施態様において、前記検証値は、検証対象となるコンテンツおよびヘッダ情報等のコンテンツ関連データを構成する部分データをメッセージとして D E S 暗号処理によって生成されるメッセージ認証

符号 (MAC) に基づいて生成されるデータであることを特徴とする。

【0028】

さらに、本発明の第3の側面は、

記憶装置に格納されるコンテンツの検証値を生成してコンテンツに対応付けて格納し、コンテンツ改竄の有無を前記検証値により実行するデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

検証値を、コンテンツのカテゴリ毎に独立した検証値として生成して格納するステップを有することを特徴とするプログラム提供媒体にある。

【0029】

なお、本発明の第3の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0030】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0031】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0032】

【発明の実施の形態】

〔システム概要〕

図1に本発明のデータ処理システムの適用可能なコンテンツ配信システム例を

示す。コンテンツ配信手段 1 0 は、データ処理手段 2 0 に対して、コンテンツあるいはコンテンツキー、その他、認証処理キー等のデータを暗号化して送信する。データ処理手段 2 0 では、受信した暗号化コンテンツ、あるいは暗号化コンテンツキー等を復号してコンテンツあるいはコンテンツキー等を取得して、画像データ、音声データの再生、あるいは各種プログラムを実行する。コンテンツの配信手段 1 0 とデータ処理手段 2 0 との間のデータ交換は、インターネット等のネットワークを介して、あるいは DVD、CD、その他の流通可能な記憶媒体を介して実行される。

【 0 0 3 3 】

データ処理手段 2 0 は、例えばフラッシュメモリ等の記憶手段を備えたメモリーカード等のデータ記憶手段 3 0 にデータを格納して保存する。データ記憶手段 3 0 には、暗号処理機能を有する記憶手段としての例えばメモリーカード（具体例としてはメモリスティック (Memory Stick: 商標)）が含まれる。データ処理手段 2 0 からデータ記憶手段 3 0 に対するデータ格納処理、およびデータ記憶手段 3 0 からデータ処理手段に対するデータ移動の際には、相互認証処理、およびデータの暗号処理が実行され不正なデータコピーの防止が図られる。

【 0 0 3 4 】

なお、データ処理手段 2 0 に含まれる各機器間でのコンテンツデータの移動も可能であり、この際にも機器間の相互認証処理、データの暗号処理が実行される。

【 0 0 3 5 】

コンテンツ配信手段 1 0 としては、インターネット 1 1、衛星放送 1 2、電話回線 1 3、DVD、CD等のメディア 1 4 等があり、一方、データ処理手段 2 0 のデバイスとしては、パーソナルコンピュータ (PC) 2 1、ポータブルデバイス (PD) 2 2、携帯電話、PDA (Personal Digital Assistants) 等の携帯機器 2 3、DVD、CDプレーヤ等の記録再生器、ゲーム端末 2 4、メモリーカード (ex. メモリスティック (商標)) を利用した再生装置 2 5 等がある。これらデータ処理手段 2 0 の各デバイスは、コンテンツ配信手段 1 0 から提供されるコンテンツをネットワーク等の通信手段あるいは、他のデータ処理手段、ま

たは、データ記憶手段 3 0 から取得可能である。

【 0 0 3 6 】

図 2 に、代表的なコンテンツデータの移動処理例を示す。図 2 に示すシステムは、パーソナルコンピュータ（PC）1 0 0、再生装置 2 0 0 および記憶装置 3 0 0 間でのデータ（コンテンツ）の移動処理例を示した図である。PC 1 0 0 は、プログラムおよびデータ記憶用のハードディスク（HD）を有し、さらに、外部記憶媒体としての CD、DVD 等を装着可能な構成を持つ。

【 0 0 3 7 】

パーソナルコンピュータ（PC）1 0 0 は、インターネット、公衆回線等の各種ネットワークに接続可能であり、例えば、EMD (Electronic Music Distribution: 電子音楽配信) などのサービスを提供する図示しないサービスプロバイダのホストコンピュータから、ネットワークをしてオーディオデータ、画像データ、プログラム等の各種データを受信し、受信したデータを必要に応じて復号して、再生装置 2 0 0 に出力する。また、パーソナルコンピュータ（PC）1 0 0 は、コンテンツデータを受信するに当たって、必要に応じて、サービスプロバイダのホストコンピュータとの間で認証処理および課金処理などを行う。また、パーソナルコンピュータ（PC）1 0 0 は、例えば、CD、DVD から入力したデータを再生装置 2 0 0 に出力する。

【 0 0 3 8 】

記憶装置 3 0 0 は、再生装置 2 0 0 に対して着脱自在な装置、例えばメモリスティック (Memory Stick: 商標) であり、フラッシュメモリなどの書き換え可能な半導体メモリを内蔵している。

【 0 0 3 9 】

図 2 に示すように、PC 1 0 0、再生装置 2 0 0、記憶装置 3 0 0 間におけるデータ移動、例えば音楽データ、画像データ等のデータ再生、データ記録、データコピー等の処理の際にはデータ移動機器間において、相互認証処理が実行され、不正な機器を用いたデータ移動は防止される。これらの処理については後述する。また、コンテンツデータのネットワークまたは各種記憶媒体を介する配信、また、PC と再生装置相互間、あるいは再生装置とメモリカード等の記憶装置間

でのコンテンツ移動の際にはコンテンツを暗号化することでデータのセキュリティが保全される。

【0040】

〔キー配信構成としてのツリー（木）構造について〕

上述のようなコンテンツに対する暗号処理に適用する暗号鍵、例えばコンテンツの暗号処理に適用するコンテンツキー、またはコンテンツキーを暗号化するためのコンテンツキー暗号化キー等の様々な暗号処理キーを、安全に正当なライセンスを持つデバイスに配信する構成として、階層キー・ツリー構成について図3以下を用いて説明する。

【0041】

図3の最下段に示すナンバ0～15がコンテンツデータの再生、実行を行なうデータ処理手段20を構成する個々のデバイス、例えばコンテンツ（音楽データ）再生装置である。すなわち図3に示す階層ツリー（木）構造の各葉（リーフ：leaf）がそれぞれのデバイスに相当する。

【0042】

各デバイス0～15は、製造時あるいは出荷時、あるいはその後において、図3に示す階層ツリー（木）構造における、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセットをメモリに格納する。図3の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフキーであり、最上段のKR（ルートキー）から、最下段から2番目の節（ノード）に記載されたキー：KR～K111をノードキーとする。

【0043】

図3に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー：K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図3のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また

、ツリーの各部において異なる段数構成を持つことが可能である。

【 0 0 4 4 】

また、図 3 のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたフラッシュメモリ等を使用したメモリカード、DVD、CD、MD等、様々なタイプの記憶装置を利用可能なデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図 3 に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【 0 0 4 5 】

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図 3 の点線で囲んだ部分、すなわちデバイス 0, 1, 2, 3 を同一の記録媒体を用いる 1 つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図 3 の点線で囲んだ部分、すなわちデバイス 0, 1, 2, 3 を 1 つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図 3 のツリー中に複数存在する。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

【 0 0 4 6 】

なお、ノードキー、リーフキーは、ある 1 つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が

実行する。

【0047】

このツリー構造において、図3から明らかなように、1つのグループに含まれる3つのデバイス0, 1, 2, 3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のコンテンツキーをデバイス0, 1, 2, 3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス0, 1, 2, 3のみに共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーKconをノードキーK00で暗号化した値Enc(K00, Kcon)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kcon)を解いてコンテンツキー：Kconを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

【0048】

また、ある時点tにおいて、デバイス3の所有する鍵：K0011, K001, K00, K0, KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0, 1, 2, 3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー：K001, K00, K0, KRをそれぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代（Generation）：tの更新キーであることを示す。

【0049】

更新キーの配布処理について説明する。キーの更新は、例えば、図4（A）に示す有効化キープロック（EKB：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス0, 1, 2に供給することによって実行される。なお、有効化キ

ーブロック (EKB) は、図3に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック (EKB) は、キー更新ブロック (KRB: Key Renewal Block) と呼ばれることもある。

【0050】

図4 (A) に示す有効化キーブロック (EKB) には、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図4の例は、図3に示すツリー構造中のデバイス0, 1, 2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータである。図3から明らかなように、デバイス0, デバイス1は、更新ノードキーとして $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要であり、デバイス2は、更新ノードキーとして $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要である。

【0051】

図4 (A) のEKBに示されるようにEKBには複数の暗号化キーが含まれる。最下段の暗号化キーは、 $Enc(K0010, K(t)001)$ である。これはデバイス2の持つリーフキー $K0010$ によって暗号化された更新ノードキー $K(t)001$ であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t)001$ を得ることができる。また、復号により得た $K(t)001$ を用いて、図4 (A) の下から2段目の暗号化キー $Enc(K(t)001, K(t)00)$ を復号可能となり、更新ノードキー $K(t)00$ を得ることができる。以下順次、図4 (A) の上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図4 (A) の上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。一方、デバイス $K0000$ 、 $K0001$ は、ノードキー $K000$ は更新する対象に含まれておらず、更新ノードキーとして必要なのは、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ である。デバイス $K0000$ 、 $K0001$ は、図4 (A) の上から3段目の暗号化キー $Enc(K000, K(t)00)$ を復号し $K(t)00$ 、を取得し、以下、図4 (A) の上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ を得る。以下順次、図4 (A) の上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し、更新ノードキー $K(t)R$ を得る。

K (t) 0 0, K (t) 0) を復号し、更新ノードキー K (t) 0、図 4 (A) の上から 1 段目の暗号化キー E n c (K (t) 0, K (t) R) を復号し K (t) R を得る。このようにして、デバイス 0, 1, 2 は更新した鍵 K (t) 0 0 1, K (t) 0 0, K (t) 0, K (t) R を得ることができる。なお、図 4 (A) のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【 0 0 5 2 】

図 3 に示すツリー構造の上位段のノードキー：K (t) 0, K (t) R の更新が不要であり、ノードキー K 0 0 のみの更新処理が必要である場合には、図 4 (B) の有効化キーブロック (E K B) を用いることで、更新ノードキー K (t) 0 0 をデバイス 0, 1, 2 に配布することができる。

【 0 0 5 3 】

図 4 (B) に示す E K B は、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図 3 に点線で示すグループ内のデバイス 0, 1, 2, 3 がある記録媒体を用いており、新たな共通のコンテンツキー K (t) c o n が必要であるとする。このとき、デバイス 0, 1, 2, 3 の共通のノードキー K 0 0 を更新した K (t) 0 0 を用いて新たな共通の更新コンテンツキー：K (t) c o n を暗号化したデータ E n c (K (t), K (t) c o n) を図 4 (B) に示す E K B とともに配布する。この配布により、デバイス 4 など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【 0 0 5 4 】

すなわち、デバイス 0, 1, 2 は E K B を処理して得た K (t) 0 0 を用いて上記暗号文を復号すれば、t 時点でのコンテンツキー K (t) c o n を得ることが可能になる。

【 0 0 5 5 】

[E K B を使用したコンテンツキーの配布]

図 5 に、t 時点でのコンテンツキー K (t) c o n を得る処理例として、K (t) 0 0 を用いて新たな共通のコンテンツキー K (t) c o n を暗号化したデー

タ $Enc(K(t)00, K(t)con)$ と図 4 (B) に示す EKB とを記録媒体を介して受領したデバイス 0 の処理を示す。すなわち EKB による暗号化メッセージデータをコンテンツキー $K(t)con$ とした例である。

【0056】

図 5 に示すように、デバイス 0 は、記録媒体に格納されている世代: t 時点の EKB と自分があらかじめ格納しているノードキー $K000$ を用いて上述したと同様の EKB 処理により、ノードキー $K(t)00$ を生成する。さらに、復号した更新ノードキー $K(t)00$ を用いて更新コンテンツキー $K(t)con$ を復号して、後にそれを使用するために自分だけが持つリーフキー $K0000$ で暗号化して格納する。

【0057】

[EKB のフォーマット]

図 6 に有効化キープブロック (EKB) のフォーマット例を示す。バージョン 601 は、有効化キープブロック (EKB) のバージョンを示す識別子である。なお、バージョンは最新の EKB を識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キープブロック (EKB) の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ 603 は、有効化キープブロック (EKB) 中のデータ部の位置を示すポインタであり、タグポインタ 604 はタグ部の位置、署名ポインタ 605 は署名の位置を示すポインタである。

【0058】

データ部 606 は、例えば更新するノードキーを暗号化したデータを格納する。例えば図 5 に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【0059】

タグ部 607 は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図 7 を用いて説明する。図 7 では、データとして先に図 4 (A) で説明した有効化キープブロック (EKB) を送付する例を示している。この時のデータは、図 7 の表 (b) に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノード

アドレスとする。この場合は、ルートキーの更新キー $K(t)R$ が含まれているので、トップノードアドレスは KR となる。このとき、例えば最上段のデータ $Enc(K(t)0, K(t)R)$ は、図 7 の (a) に示す階層ツリーに示す位置にある。ここで、次のデータは、 $Enc(K(t)00, K(t)0)$ であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが 0、ない場合は 1 が設定される。タグは {左 (L) タグ, 右 (R) タグ} として設定される。最上段のデータ $Enc(K(t)0, K(t)R)$ の左にはデータがあるので、L タグ = 0、右にはデータがないので、R タグ = 1 となる。以下、すべてのデータにタグが設定され、図 7 (c) に示すデータ列、およびタグ列が構成される。

【0060】

タグは、データ $Enc(Kxxx, Kyyy)$ がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータ $Enc(Kxxx, Kyyy) \dots$ は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図 4 で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

0 : $Enc(K(t)0, K(t)root)$

00 : $Enc(K(t)00, K(t)0)$

000 : $Enc(K((t)000, K(T)00)$

...

のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【0061】

図 6 に戻って、EKB フォーマットについてさらに説明する。署名 (Signatur

e) は、有効化キープロック (EKB) を発行した例えば鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。EKB を受領したデバイスは署名検証によって正当な有効化キープロック (EKB) 発行者が発行した有効化キープロック (EKB) であることを確認する。

【 0 0 6 2 】

[EKB を使用したコンテンツキーおよびコンテンツの配信]

上述の例では、コンテンツキーのみを EKB とともに送付する例について説明したが、コンテンツキーで暗号化したコンテンツと、コンテンツキー暗号キーで暗号化したコンテンツキーと、EKB によって暗号化したコンテンツキー暗号キーを併せて送付する構成について以下説明する。

【 0 0 6 3 】

図 8 にこのデータ構成を示す。図 8 (a) に示す構成において、Enc (Kcon, content) 801 は、コンテンツ (Content) をコンテンツキー (Kcon) で暗号化したデータであり、Enc (KEK, Kcon) 802 は、コンテンツキー (Kcon) をコンテンツキー暗号キー (KEK : Key Encryption Key) で暗号化したデータであり、Enc (EKB, KEK) 803 は、コンテンツキー暗号キー KEK を有効化キープロック (EKB) によって暗号化したデータであることを示す。

【 0 0 6 4 】

ここで、コンテンツキー暗号キー KEK は、図 3 で示すノードキー (K000, K00...)、あるいはルートキー (KR) 自体であってもよく、またノードキー (K000, K00...)、あるいはルートキー (KR) によって暗号化されたキーであってもよい。

【 0 0 6 5 】

図 8 (b) は、複数のコンテンツがメディアに記録され、それぞれが同じ Enc (EKB, KEK) 805 を利用している場合の構成例を示す、このような構成においては、各データに同じ Enc (EKB, KEK) を付加することなく、Enc (EKB, KEK) にリンクするリンク先を示すデータを各データに付加する構成とすることができる。

【 0 0 6 6 】

図 9 にコンテンツキー暗号キー KEK を、図 3 に示すノードキー $K00$ を更新した更新ノードキー $K(t)00$ として構成した場合の例を示す。この場合、図 3 の点線枠で囲んだグループにおいてデバイス 3 が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス 0, 1, 2 に対して図 9 に示す (a) 有効化キープロック (EKB) と、(b) コンテンツキー ($Kcon$) をコンテンツキー暗号キー ($KEK = K(t)00$) で暗号化したデータと、(c) コンテンツ ($content$) をコンテンツキー ($Kcon$) で暗号化したデータとを配信することにより、デバイス 0, 1, 2 はコンテンツを得ることができる。

【 0 0 6 7 】

図 9 の右側には、デバイス 0 における復号手順を示してある。デバイス 0 は、まず、受領した有効化キープロックから自身の保有するリーフキー $K000$ を用いた復号処理により、コンテンツキー暗号キー ($KEK = K(t)00$) を取得する。次に、 $K(t)00$ による復号によりコンテンツキー $Kcon$ を取得し、さらにコンテンツキー $Kcon$ によりコンテンツの復号を行なう。これらの処理により、デバイス 0 はコンテンツを利用可能となる。デバイス 1, 2 においても各々異なる処理手順で EKB を処理することにより、コンテンツキー暗号キー ($KEK = K(t)00$) を取得することが可能となり、同様にコンテンツを利用することが可能となる。

【 0 0 6 8 】

図 3 に示す他のグループのデバイス 4, 5, 6... は、この同様のデータ (EKB) を受信したとしても、自身の保有するリーフキー、ノードキーを用いてコンテンツキー暗号キー ($KEK = K(t)00$) を取得することができない。同様にリボークされたデバイス 3 においても、自身の保有するリーフキー、ノードキーでは、コンテンツキー暗号キー ($KEK = K(t)00$) を取得することができず、正当な権利を有するデバイスのみがコンテンツを復号して利用することが可能となる。

【 0 0 6 9 】

このように、E K B を利用したコンテンツキーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした暗号化コンテンツを配信することが可能となる。

【 0 0 7 0 】

なお、有効化キーブロック (E K B)、コンテンツキー、暗号化コンテンツ等は、ネットワークを介して安全に配信することが可能な構成であるが、有効化キーブロック (E K B)、コンテンツキー、暗号化コンテンツを D V D、C D 等の記録媒体に格納してユーザに提供することも可能である。この場合、記録媒体に格納された暗号化コンテンツの復号には、同一の記録媒体に格納された有効化キーブロック (E K B) の復号により得られるコンテンツキーを使用するように構成すれば、予め正当権利者のみが保有するリーフキー、ノードキーによってのみ利用可能な暗号化コンテンツの配布処理、すなわち利用可能なユーザデバイスを限定したコンテンツ配布が簡易な構成で実現可能となる。

【 0 0 7 1 】

図 1 0 に記録媒体に暗号化コンテンツとともに有効化キーブロック (E K B) を格納した構成例を示す。図 1 0 に示す例においては、記録媒体にコンテンツ C 1 ~ C 4 が格納され、さらに各格納コンテンツに対応するの有効化キーブロック (E K B) を対応付けたデータが格納され、さらにバージョン M の有効化キーブロック (E K B __ M) が格納されている。例えば E K B __ 1 はコンテンツ C 1 を暗号化したコンテンツキー K c o n 1 を生成するのに使用され、例えば E K B __ 2 はコンテンツ C 2 を暗号化したコンテンツキー K c o n 2 を生成するのに使用される。この例では、バージョン M の有効化キーブロック (E K B __ M) が記録媒体に格納されており、コンテンツ C 3, C 4 は有効化キーブロック (E K B __ M) に対応付けられているので、有効化キーブロック (E K B __ M) の復号によりコンテンツ C 3, C 4 のコンテンツキーを取得することができる。E K B __ 1、E K B __ 2 はディスクに格納されていないので、新たな提供手段、例えばネットワーク配信、あるいは記録媒体による配信によってそれぞれのコンテンツキーを復号するために必要な E K B __ 1, E K B __ 2 を取得することが必要となる。

【 0 0 7 2 】

〔階層ツリー構造のカテゴリ分類〕

暗号鍵をルートキー、ノードキー、リーフキー等、図3の階層ツリー構造として構成し、コンテンツキー、認証キー、ICV生成キー、あるいはプログラムコード、データ等を有効化キーブロック（EKB）とともに暗号化して配信する構成について説明してきたが、ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリ毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

【0073】

図11に階層ツリー構造のカテゴリの分類の一例を示す。図11において、階層ツリー構造の最上段には、ルートキーK r o o t 1 1 0 1が設定され、以下の中間段にはノードキー1 1 0 2が設定され、最下段には、リーフキー1 1 0 3が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

【0074】

ここで、一例として最上段から第M段目のあるノードをカテゴリノード1 1 0 4として設定する。すなわち第M段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第M段の1つのノードを頂点として以下、M+1段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。

【0075】

例えば図11の第M段目の1つのノード1 1 0 5にはカテゴリ〔メモリスティック（商標）〕が設定され、このノード以下に連なるノード、リーフはメモリスティックを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード1 1 0 5以下を、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義する。

【0076】

さらに、M段から数段分下位の段をサブカテゴリノード1 1 0 6として設定することができる。例えば図に示すようにカテゴリ〔メモリスティック〕ノード1 1 0 5の2段下のノードに、メモリスティックを使用したデバイスのカテゴリに

含まれるサブカテゴリノードとして、[再生専用器]のノードを設定する。さらに、サブカテゴリノードである再生専用器のノード1106以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード1107が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる[PHS]ノード1108と[携帯電話]ノード1109を設定することができる。

【0077】

さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば1つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器XYZ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器XYZにその頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（EKB）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【0078】

このように、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（EKB）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

【0079】

[簡略EKBによるキー配信構成]

先に説明した例えば図3のツリー構成において、キー、例えばコンテンツキーを所定デバイス（リーフ）宛に送付する場合、キー配布先デバイスの所有してい

るリーフキー、ノードキーを用いて復号可能な有効化キープブロック (EKB) を生成して提供する。例えば図 1 2 (a) に示すツリー構成において、リーフを構成するデバイス a, g, j に対してキー、例えばコンテンツキーを送信する場合、a, g, j の各ノードにおいて復号可能な有効化キープブロック (EKB) を生成して配信する。

【0080】

例えば更新ルートキー $K(t)_{root}$ でコンテンツキー $K(t)_{con}$ を暗号化处理し、EKB とともに配信する場合を考える。この場合、デバイス a, g, j は、それぞれが図 1 2 (b) に示すリーフおよびノードキーを用いて、EKB の処理を実行して $K(t)_{root}$ を取得し、取得した更新ルートキー $K(t)_{root}$ によってコンテンツキー $K(t)_{con}$ の復号処理を実行してコンテンツキーを得る。

【0081】

この場合に提供される有効化キープブロック (EKB) の構成は、図 1 3 に示すようになる。図 1 3 に示す有効化キープブロック (EKB) は、先の図 6 で説明した有効化キープブロック (EKB) のフォーマットにしたがって構成されたものであり、データ (暗号化キー) と対応するタグとを持つ。タグは、先に図 7 を用いて説明したように左 (L)、右 (R)、それぞれの方向にデータがあれば 0、無ければ 1 を示している。

【0082】

有効化キープブロック (EKB) を受領したデバイスは、有効化キープブロック (EKB) の暗号化キーとタグに基づいて、順次暗号化キーの復号処理を実行して上位ノードの更新キーを取得していく。図 1 3 に示すように、有効化キープブロック (EKB) は、ルートからリーフまでの段数 (デプス) が多いほど、そのデータ量は増加していく。段数 (デプス) は、デバイス (リーフ) 数に応じて増大するものであり、キーの配信先となるデバイス数が多い場合は、EKB のデータ量がさらに増大することになる。

【0083】

このような有効化キープブロック (EKB) のデータ量の削減を可能とした構成

について説明する。図 1 4 は、有効化キーブロック (E K B) をキー配信デバイスに応じて簡略化して構成した例を示すものである。

【 0 0 8 4 】

図 1 3 と同様、リーフを構成するデバイス a, g, j に対してキー、例えばコンテンツキーを送信する場合を想定する。図 1 4 の (a) に示すように、キー配信デバイスによってのみ構成されるツリーを構築する。この場合、図 1 2 (b) に示す構成に基づいて新たなツリー構成として図 1 4 (b) のツリー構成が構築される。K r o o t から K j までは全く分岐がなく 1 つの枝のみが存在すればよく、K r o o t から K a および K g に至るためには、K 0 に分岐点を構成するのみで、2 分岐構成の図 1 4 (a) のツリーが構築される。

【 0 0 8 5 】

図 1 4 (a) に示すように、ノードとして K 0 のみを持つ簡略化したツリーが生成される。更新キー配信のための有効化キーブロック (E K B) は、これらの簡略ツリーに基づいて生成する。図 1 4 (a) に示すツリーは、有効化キーブロック (E K B) を復号可能な末端ノードまたはリーフを最下段とした 2 分岐型ツリーを構成するパスを選択して不要ノードを省略することにより再構築される再構築階層ツリーである。更新キー配信のための有効化キーブロック (E K B) は、この再構築階層ツリーのノードまたはリーフに対応するキーのみに基づいて構成される。

【 0 0 8 6 】

先の図 1 3 で説明した有効化キーブロック (E K B) は、各リーフ a, g, j から K r o o t に至るまでのすべてのキーを暗号化したデータを格納していたが、簡略化 E K B は、簡略化したツリーを構成するノードについてのみの暗号化データを格納する。図 1 4 (b) に示すようにタグは 3 ビット構成を有する。第 1 および第 2 ビットは、図 1 3 の例と、同様の意味を持ち、左 (L)、右 (R)、それぞれの方向にデータがあれば 0、無ければ 1 を示す。第 3 番目のビットは、E K B 内に暗号化キーが格納されているか否かを示すためのビットであり、データが格納されている場合は 1、データが無い場合は、0 として設定される。

【 0 0 8 7 】

データ通信網、あるいは記憶媒体に格納されてデバイス（リーフ）に提供される有効化キープロック（EKB）は、図14（b）に示すように、図13に示す構成に比較すると、データ量が大幅に削減されたものとなる。図14に示す有効化キープロック（EKB）を受領した各デバイスは、タグの第3ビットに1が格納された部分のデータのみを順次復号することにより、所定の暗号化キーの復号を実現することができる。例えばデバイスaは、暗号化データ $Enc(K_a, K(t)_0)$ をリーフキー K_a で復号して、ノードキー $K(t)_0$ を取得して、ノードキー $K(t)_0$ によって暗号化データ $Enc(K(t)_0, K(t)_{root})$ を復号して $K(t)_{root}$ を取得する。デバイスjは、暗号化データ $Enc(K_j, K(t)_{root})$ をリーフキー K_j で復号して、 $K(t)_{root}$ を取得する。

【0088】

このように、配信先のデバイスによってのみ構成される簡略化した新たなツリー構成を構築して、構築されたツリーを構成するリーフおよびノードのキーのみを用いて有効化キープロック（EKB）を生成することにより、少ないデータ量の有効化キープロック（EKB）を生成することが可能となり、有効化キープロック（EKB）のデータ配信が効率的に実行可能となる。

【0089】

なお、簡略化した階層ツリー構成は、後段で説明するエンティティ単位のEKB管理構成において特に有効に活用可能である。エンティティは、キー配信構成としてのツリー構成を構成するノードあるいはリーフから選択した複数のノードあるいはリーフの集合体ブロックである。エンティティは、デバイスの種類に応じて設定される集合であったり、あるいはデバイス提供メーカー、コンテンツプロバイダ、決済機関等の管理単位等、ある共通点を持った処理単位、管轄単位、あるいは提供サービス単位等、様々な態様の集合として設定される。1つのエンティティには、ある共通のカテゴリに分類されるデバイスが集まっており、例えば複数のエンティティの頂点ノード（サブルート）によって上述したと同様の簡略化したツリーを再構築してEKBを生成することにより、選択されたエンティティに属するデバイスにおいて復号可能な簡略化された有効化キープロック（E

K B) の生成、配信が可能となる。エンティティ単位の管理構成については後段で詳細に説明する。

【 0 0 9 0 】

なお、このような有効化キープブロック (E K B) は、光ディスク、DVD等の情報記録媒体に格納した構成とすることが可能である。例えば、上述の暗号化キーデータによって構成されるデータ部と、暗号化キーデータの階層ツリー構造における位置識別データとしてのタグ部とを含む有効化キープブロック (E K B) にさらに、更新ノードキーによって暗号化したコンテンツ等のメッセージデータとを格納した情報記録媒体を各デバイスに提供する構成が可能である。デバイスは有効化キープブロック (E K B) に含まれる暗号化キーデータをタグ部の識別データにしたがって順次抽出して復号し、コンテンツの復号に必要なキーを取得してコンテンツの利用を行なうことが可能となる。もちろん、有効化キープブロック (E K B) をインターネット等のネットワークを介して配信する構成としてもよい。

【 0 0 9 1 】

[暗号処理機能を有する記憶装置とデータ処理装置間のデータ移動]

次に、上述した階層ツリー構成を適用した有効化キープブロック (E K B) によって配信される暗号処理キーを適用した処理構成について、暗号処理機能を有する記憶装置、例えばメモリスティック (商標) 等のメモリカードと、データ再生装置間におけるデータ移動処理を中心として説明する。

【 0 0 9 2 】

図 1 5 は、相互にコンテンツデータの移動を実行可能な再生装置と暗号処理機能を有するメモリカード等の記憶装置の詳細構成を示したブロック図である。

【 0 0 9 3 】

図 1 5 に示すように、記憶装置 3 0 0 は、例えば、主制御モジュール 3 1、通信インターフェイス 3 2、制御モジュール 3 3、フラッシュメモリ 3 4 およびフラッシュメモリ管理モジュール 3 5 を有する。以下、各モジュールについて説明する。

【 0 0 9 4 】

〔制御モジュール 3 3〕

図 1 5 に示すように、制御モジュール 3 3 は、例えば、乱数発生ユニット 5 0、記憶ユニット 5 1、鍵生成／演算ユニット 5 2、相互認証ユニット 5 3、暗号化／復号ユニット 5 4 および制御ユニット 5 5 を有する。制御モジュール 3 3 は、シングルチップの暗号処理専用の集積回路であり、多層構造を有し、内部のメモリセルはアルミニウム層などのダミー層に挟まれている。また、制御モジュール 3 3 は、動作電圧または動作周波数の幅が狭く、外部から不正にデータを読み出せないように耐タンパー性を有している。乱数発生ユニット 5 0 は、乱数発生指示を受けると、6 4 ビット（8 バイト）の乱数を発生する。

〔0 0 9 5〕

記憶ユニット 5 1 は、例えば、EEPROM(Electrically Erasable Programmable Read Only Memory) などの不揮発性メモリであり、認証処理に必要な鍵データなどの種々のデータを記憶している。図 1 6 は、記憶ユニット 5 1 に記憶されているデータを説明するための図である。図 1 6 に示すように、記憶ユニット 5 1 は、認証鍵データ I K 0 ～ I K 31、装置識別データ I D m および記憶用鍵データ K s t r を記憶している。

〔0 0 9 6〕

認証鍵データ I K 0 ～ I K 31 は、記憶装置 3 0 0 が再生装置 2 0 0 との間で相互認証を行う際に用いられる鍵データであり、後述するように相互認証を行う度に認証鍵データ I K 0 ～ I K 31 のうちの認証鍵データがランダムに選択される。なお、認証鍵データ I K 0 ～ I K 31 および記憶用鍵データ K s t r は、記憶装置 3 0 0 の外部から読めないようになっている。装置識別データ I D m は、記憶装置 3 0 0 に対してユニークに付けられた識別データであり、後述するように、記憶装置 3 0 0 が再生装置 2 0 0 との間で相互認証を行う際に読み出されて再生装置 2 0 0 に出力される。記憶用鍵データ K s t r は、後述するように、コンテンツの暗号化に用いられるコンテンツ鍵データ C K を暗号化してフラッシュメモリ 3 4 に記憶する際に用いられる。

〔0 0 9 7〕

鍵生成／演算ユニット 5 2 は、例えば、ISO/IEC 9 7 9 7 の MAC (Mes

sage Authentication Code) 演算などの種々の演算を行って鍵データを生成する。このとき、MAC演算には、例えば、“Block cipher Algorithm”としてFIPS PUB 46-2に規定されるDES (Data Encryption Standard)が用いられる。MAC演算は、任意の長さのデータを固定の長さに圧縮する一方向性ハッシュ関数演算であり、関数値が秘密鍵に依存して定まる。

【0098】

相互認証ユニット53は、再生装置200からオーディオデータを入力してフラッシュメモリ34に書き込む動作を行うのに先立って、再生装置200との間で相互認証処理を行う。また、相互認証ユニット53は、フラッシュメモリ34からオーディオデータを読み出して再生装置200に出力する動作を行うのに先立って、再生装置200との間で相互認証処理を行う。また、相互認証ユニット53は、相互認証処理において、前述したMAC演算を行う。当該相互認証処理では、記憶ユニット51に記憶されているデータが用いられる。

【0099】

暗号化／復号ユニット54は、DES、IDEA、MISTYなどのブロック暗号アルゴリズムでの暗号化を行う。使用するモードは、FIPS PUB 81 “DES MODES OF OPERATION”に規定されているようなECB (Electronic Code Book)モードおよびCBC (Cipher Block Chaining) モードである。また、暗号化／復号ユニット54は、DES、IDEA、MISTYなどのブロック復号アルゴリズムでの復号を行う。使用するモードは、上記ECBモードおよびCBCモードである。当該ECBモードおよびCBCモードのブロック暗号化／復号では、指定された鍵データを用いて指定されたデータを暗号化／復号する。制御ユニット55は、乱数発生ユニット50、記憶ユニット51、鍵生成／演算ユニット52、相互認証ユニット53および暗号化／復号ユニット54の処理を統括して制御する。

【0100】

〔フラッシュメモリ34〕

フラッシュメモリ34は、例えば、32Mバイトの記憶容量を有する。フラッシュメモリ34には、相互認証ユニット53による再生装置200と記憶装置3

00との間の相互認証処理によって双方が正当な装置であると認められたときに、再生装置200から入力したオーディオデータあるいは画像データ等、各種データが書き込まれる。また、フラッシュメモリ34からは、相互認証ユニット53による再生装置200と記憶装置300との間の相互認証処理によって正当な相手であると認められたときに、オーディオデータ、画像データ等が読み出されて再生装置200に出力される。

【0101】

以下、フラッシュメモリ34に記憶されるデータおよびそのフォーマットについて説明する。図17は、フラッシュメモリ34に記憶されるデータを説明するための図である。図17に示すように、フラッシュメモリ34には、例えば、再生管理ファイル、複数のトラックデータ（再生データ）ファイルが記憶されている。ここで、再生管理ファイルはトラックデータファイルの再生を管理する管理データを有し、トラックデータファイルはそれぞれ対応するトラックデータ（オーディオデータ）を有している。なお、本実施形態では、トラックデータは、例えば、1曲分のオーディオデータを意味する。以下、フラッシュメモリ34に記憶されるデータをオーディオデータとした場合の例について説明する。

【0102】

図18は、再生管理ファイルの構成を示し、図19が一つ（1曲）のATRAC3データファイルの構成を示す。再生管理ファイルは、16KB固定長のファイルである。ATRAC3データファイルは、曲単位でもって、先頭の属性ヘッダと、それに続く実際の暗号化された音楽データとからなる。属性ヘッダも16KB固定長とされ、再生管理ファイルと類似した構成を有する。

【0103】

再生管理ファイルは、ヘッダ、1バイトコードのメモリカードの名前NM1-S、2バイトコードのメモリカードの名前NM2-S、曲順の再生テーブルTRKTBL、メモリカード全体の付加情報INF-Sとからなる。データファイルの先頭の属性ヘッダは、ヘッダ、1バイトコードの曲名NM1、2バイトコードの曲名NM2、トラックのキー情報等のトラック情報TRKINF、パーツ情報PRTINFと、トラックの付加情報INFとからなる。ヘッダには、総パーツ

数、名前の属性、付加情報のサイズの情報等が含まれる。

【0104】

属性ヘッダに対してATRAC3の音楽データが続く。音楽データは、16KBのブロック毎に区切られ、各ブロックの先頭にヘッダが付加されている。ヘッダには、暗号を復号するための初期値が含まれる。なお、暗号化の処理を受けるのは、ATRAC3データファイル中の音楽データ等のコンテンツデータのみであって、それ以外の再生管理ファイル、ヘッダ等のデータは、暗号化されない。

【0105】

図20に、ATRAC3データファイルA3Dnnnnのデータ配列例を示す。図20には、データファイルの属性ヘッダ（1ブロック）と、音楽データファイル（1ブロック）とが示されている。図20では、この2ブロック（16×2＝32Kバイト）の各スロットの先頭のバイト（0x0000～0x7FF0）が示されている。図21に分離して示すように、属性ヘッダの先頭から32バイトがヘッダであり、256バイトが曲名領域NM1（256バイト）であり、512バイトが曲名領域NM2（512バイト）である。属性ヘッダのヘッダには、下記のデータが書かれる。

【0106】

BLKID-HD0（4バイト）

意味：BLOCKID FILE ID

機能：ATRAC3データファイルの先頭であることを識別するための値

値：固定値＝”HD＝0”（例えば0x48442D30）

【0107】

MCODE（2バイト）

意味：MAKER CODE

機能：記録した機器の、メーカー、モデルを識別するコード

値：上位10ビット（メーカーコード） 下位6ビット（機種コード）

【0108】

BLOCK SERIAL（4バイト）

意味：トラック毎に付けられた連続番号

機能：ブロックの先頭は 0 から始まり次のブロックは + 1 づつインクリメント
編集されても値を変化させない

値：0 より始まり 0 x F F F F F F F F まで。

【 0 1 0 9 】

N 1 C + L (2 バイト)

意味：トラック (曲名) データ (N M 1) の属性を表す

機能：N M 1 に使用される文字コードと言語コードを各 1 バイトで表す

値：S N 1 C + L と同一

【 0 1 1 0 】

N 2 C + L (2 バイト)

意味：トラック (曲名) データ (N M 2) の属性を表す

機能：N M 2 に使用される文字コードと言語コードを各 1 バイトで表す

値：S N 1 C + L と同一

【 0 1 1 1 】

I N F S I Z E (2 バイト)

意味：トラックに関する付加情報の全てを合計したサイズを表す

機能：データサイズを 1 6 バイト単位の大きさを記述、無い場合は必ずオール
ゼロとすること

値：サイズは 0 x 0 0 0 0 から 0 x 3 C 6 (9 6 6)

【 0 1 1 2 】

T - P R T (2 バイト)

意味：トータルパーツ数

機能：トラックを構成するパーツ数を表す。通常は 1

値：1 から 0 x 2 8 5 (6 4 5 dec)

【 0 1 1 3 】

T - S U (4 バイト)

意味：トータル S U (サウンドユニット) 数、S U は、パーツの最小単位であり、且つ A T R A C 3 でオーディオデータを圧縮する時の最小のデータ単位である。4 4 . 1 k H z のサンプリング周波数で得られた 1 0 2 4 サンプル分 (1 0 2

4 × 1 6 ビット × 2 チャンネル) のオーディオデータを約 1 / 1 0 に圧縮した数百バイトのデータが S U である。1 S U は、時間に換算して約 2 3 m 秒になる。通常は、数千に及ぶ S U によって 1 つのパーツが構成される。1 クラスタが 4 2 個の S U で構成される場合、1 クラスタで約 1 秒の音を表すことができる。1 つのトラックを構成するパーツの数は、付加情報サイズに影響される。パーツ数は、1 ブロックの中からヘッダや曲名、付加情報データ等を除いた数で決まるために、付加情報が全く無い状態が最大数 (6 4 5 個) のパーツを使用できる条件となる。

機能：1 トラック中の実際の総 S U 数を表す。曲の演奏時間に相当する

値：0 x 0 1 から 0 x 0 0 1 F F F F F

【 0 1 1 4 】

I N X (2 バイト) (O p t i o n)

意味：INDEX の相対場所

機能：曲のさびの部分 (特徴的な部分) の先頭を示すポインタ。曲の先頭からの位置を S U の個数を 1 / 4 した数で指定する。これは、通常の S U の 4 倍の長さの時間 (約 9 3 m 秒) に相当する

値：0 から 0 x F F F F (最大、約 6 0 8 4 秒)

【 0 1 1 5 】

X T (2 バイト) (O p t i o n)

意味：INDEX の再生時間

機能：I N X - n n n で指定された先頭から再生すべき時間の S U の個数を 1 / 4 した数で指定する。これは、通常の S U の 4 倍の長さの時間 (約 9 3 m 秒) に相当する

値：0 x 0 0 0 0 : 無設定 0 x 0 1 から 0 x F F F E (最大 6 0 8 4 秒)

0 x F F F F : 曲の終わりまで。

【 0 1 1 6 】

次に曲名領域 N M 1 および N M 2 について説明する。

【 0 1 1 7 】

N M 1

意味：曲名を表す文字列

機能：1バイトの文字コードで表した可変長の曲名（最大で256）

名前データの終了は、必ず終端コード（0x00）を書き込むこと

サイズはこの終端コードから計算すること、データの無い場合は少なくとも先頭（0x0020）からヌル（0x00）を1バイト以上記録すること

値：各種文字コード

【0118】

NM2

意味：曲名を表す文字列

機能：2バイトの文字コードで表した可変長の名前データ（最大で512）

名前データの終了は、必ず終端コード（0x00）を書き込むこと

サイズはこの終端コードから計算すること、データの無い場合は少なくとも先頭（0x0120）からヌル（0x00）を2バイト以上記録すること

値：各種文字コード。

【0119】

属性ヘッダの固定位置（0x320）から始まる、80バイトのデータをトラック情報領域TRKINFと呼び、主としてセキュリティ関係、コピー制御関係の情報を一括して管理する。図22にTRKINFの部分を示す。TRKINF内のデータについて、配置順序に従って以下に説明する。

【0120】

EKI（1バイト）

意味：前述の階層ツリー構成による有効化キープロック（EKB）によって提供される暗号化コンテンツキー：E（KEKn, Kcon）を有するか否かを示す。

機能：bit7=1でキー有、bit7=0で無し。bit7=0の場合は、EKB_version、E（KEKn, Kcon）は非参照。

値：0から0xFFまで

【0121】

EK_version（4バイト）

意味：前述の階層ツリー構成による有効化キープブロック（E K B）によって提供されるコンテンツキーの世代番号、および／または有効化キープブロック（E K B）のファイル名を示す。

機能：階層ツリー構成による有効化キープブロック（E K B）によって提供されるコンテンツキーを求めるための有効化キープブロック（E K B）を示す。

値：0 から 0 x F F まで

【0 1 2 2】

E (K s t r, K c o n) (8 バイト)

意味：コンテンツ毎の暗号処理用のキーであるコンテンツキーをメモリカードのストレージキー（K s t r）で暗号化したデータ。

機能：コンテンツの暗号処理に使用される

値：0 から 0 x F F F F F F F F F F F F F F F F まで

【0 1 2 3】

C _ M A C [n] (8 バイト)

意味：著作権情報改ざんチェック値

機能：コンテンツ累積番号を含む複数の T R K I N F の内容と隠しシーケンス番号から作成される値。隠しシーケンス番号とは、メモリカードの隠し領域に記録されているシーケンス番号のことである。著作権対応でないレコーダは、隠し領域を読むことができない。また、著作権対応の専用のレコーダ、またはメモリカードを読むことを可能とするアプリケーションを搭載したパーソナルコンピュータは、隠し領域をアクセスすることができる。

【0 1 2 4】

A (1 バイト)

意味：パーツの属性

機能：パーツ内の圧縮モード等の情報を示す

値：図 2 3 を参照して以下に説明する

ただし、N = 0, 1 のモノラルは、b i t 7 が 1 でサブ信号を 0、メイン信号（L + R）のみの特別な J o i n t モードをモノラルとして規定する。b i t 2, 1 の情報は通常の再生機は無視しても構わない。

【0125】

Aのビット0は、エンファシスのオン／オフの情報を形成し、ビット1は、再生SKIPか、通常再生かの情報を形成し、ビット2は、データ区分、例えばオーディオデータか、FAX等の他のデータかの情報を形成する。ビット3は、未定義である。ビット4、5、6を組み合わせることによって、図示のように、ATRAC3のモード情報が規定される。すなわち、Nは、この3ビットで表されるモードの値であり、モノ(N=0, 1), LP(N=2), SP(N=4), EX(N=5), HQ(N=7)の5種類のモードについて、記録時間(64MBのメモ리카ードの場合)、データ転送レート、1ブロック内のSU数がそれぞれ示されている。1SUのバイト数は、(モノ:136バイト、LP:192バイト、SP:304バイト、EX:384バイト、HQ:512バイト)である。さらに、ビット7によって、ATRAC3のモード(0: Dual 1: Joint)が示される。

【0126】

一例として、64MBのメモ리카ードを使用し、SPモードの場合について説明する。64MBのメモ리카ードには、3968ブロックがある。SPモードでは、1SUが304バイトであるので、1ブロックに53SUが存在する。1SUは、(1024/44100)秒に相当する。従って、1ブロックは、(1024/44100)×53×(3968-16)=4863秒=81分

転送レートは、

$$(44100/1024) \times 304 \times 8 = 104737 \text{ bps}$$

となる。

【0127】

LT (1バイト)

意味: 再生制限フラグ(ビット7およびビット6)とセキュリティバージョン(ビット5-ビット0)

機能: このトラックに関して制限事項があることを表す

値: ビット7: 0=制限なし 1=制限有り

ビット6: 0=期限内 1=期限切れ

ビット5ービット0：セキュリティバージョン0（0以外であれば再生禁止とする）

【0128】

FN○（2バイト）

意味：ファイル番号

機能：最初に記録された時のトラック番号、且つこの値は、メモ리카ード内の隠し領域に記録されたMAC計算用の値の位置を特定する

値：1から0x190（400）

【0129】

MG（D）SERIAL-*nnn*（16バイト（upper：8，Lower：8））

意味：記録機器のセキュリティブロック（セキュリティIC20）のシリアル番号

機能：記録機器ごとに全て異なる固有の値

値：0から0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

【0130】

CONNUM（4バイト）

意味：コンテンツ累積番号

機能：曲毎に累積されていく固有の値で記録機器のセキュリティブロックによって管理される。2の32乗、42億曲分用意されており、記録した曲の識別に使用する

値：0から0xFFFFFFFF。

【0131】

YMDhms-S（4バイト）（Option）

意味：再生制限付きのトラックの再生開始日時

機能：EMDで指定する再生開始を許可する日時

値：上述した日時の表記と同じ

YMDhms-E（4バイト）（Option）

意味：再生制限付きのトラックの再生終了日時

機能：EMDで指定する再生許可を終了する日時

値：上述した日時の表記と同じ

【0132】

MT (1バイト) (Option)

意味：再生許可回数の最大値

機能：EMDで指定される最大の再生回数

値：1から0xFF 未使用の時は、0x00

LTのbit 7の値が0の場合はMTの値は00とすること

【0133】

CT (1バイト) (Option)

意味：再生回数

機能：再生許可された回数の内で、実際に再生できる回数。再生の度にデクリメントする

値：0x00～0xFF 未使用の時は、0x00である

LTのbit 7が1でCTの値が00の場合は再生を禁止すること。

【0134】

CC (1バイト)

意味：COPY CONTROL

機能：コピー制御

値：図24に示すように、ビット6および7によってコピー制御情報を表し、ビット4および5によって高速デジタルコピーに関するコピー制御情報を表し、ビット2および3によってセキュリティブロック認証レベルを表す。ビット0および1は、未定義

CCの例：(bit 7, 6) 11：無制限のコピーを許可、01：コピー禁止、00：1回のコピーを許可 (bit 3, 2) 00：アナログないしデジタルインからの録音、MG認証レベルは0とする

CDからのデジタル録音では (bit 7, 6) は00、(bit 3, 2) は00となる

【0135】

CN (1バイト) (Option)

意味：高速デジタルコピーHSCMS (High speed Serial Copy Management System)におけるコピー許可回数

機能：コピー1回か、コピーフリーかの区別を拡張し、回数で指定する。コピー第1世代の場合にのみ有効であり、コピーごとに減算する

値：00：コピー禁止、01から0xFE：回数、0xFF：回数無制限。

【0136】

上述したトラック情報領域TRKINFに続いて、0x0370から始まる24バイトのデータをパーツ管理用のパーツ情報領域PRTINFと呼び、1つのトラックを複数のパーツで構成する場合に、時間軸の順番にPRTINFを並べていく。図25にPRTINFの部分を示す。PRTINF内のデータについて、配置順序に従って以下に説明する。

【0137】

PRTSIZE (4バイト)

意味：パーツサイズ

機能：パーツの大きさを表す。クラスタ：2バイト（最上位）、開始SU：1バイト（上位）、終了SU：1バイト（最下位）

値：クラスタ：1から0x1F40（8000）、開始SU：0から0xA0（160）、終了SU：0から0xA0（160）（但し、SUの数は、0，1，2，と0から開始する）

【0138】

PRTKEY (8バイト)

意味：パーツを暗号化するための値

機能：初期値＝0、編集時は編集の規則に従うこと

値：0から0xFFFFFFFFFFFFFFFF

【0139】

CONNUM0 (4バイト)

意味：最初に作られたコンテンツ累積番号キー

機能：コンテンツをユニークにするためのIDの役割

値：コンテンツ累積番号初期値キーと同じ値とされる。

【 0 1 4 0 】

図 2 0 に戻る。A T R A C 3 データファイルの属性ヘッダ中には、図 2 0 に示すように、付加情報 I N F が含まれる。I N F は、トラックに関する付加情報データであり、ヘッダを伴った可変長の付加情報データ。複数の異なる付加情報が並べられることがある。それぞれに I D とデータサイズが付加されている。個々のヘッダを含む付加情報データは、最小 1 6 バイト以上で 4 バイトの整数倍の単位である。

【 0 1 4 1 】

上述した属性ヘッダに対して、A T R A C 3 データファイルの各ブロックのデータが続く。図 2 6 に示すように、ブロック毎にヘッダが付加される。各ブロックのデータについて以下に説明する。

【 0 1 4 2 】

B L K I D - A 3 D (4 バイト)

意味：BLOCKID FILE ID

機能：A T R A C 3 データの先頭であることを識別するための値

値：固定値＝" A 3 D " (例えば 0 x 4 1 3 3 4 4 2 0)

【 0 1 4 3 】

M C o d e (2 バイト)

意味：MAKER CODE

機能：記録した機器の、メーカー、モデルを識別するコード

値：上位 1 0 ビット (メーカーコード) 下位 6 ビット (機種コード)

【 0 1 4 4 】

C O N N U M 0 (4 バイト)

意味：最初に作られたコンテンツ累積番号

機能：コンテンツをユニークにするための I D の役割、編集されても値は変化させない

値：コンテンツ累積番号初期値キーと同じ値とされる

【 0 1 4 5 】

BLOCK SERIAL (4 バイト)

意味：トラック毎に付けられた連続番号

機能：ブロックの先頭は 0 から始まり次のブロックは + 1 ずつインクリメント
編集されても値を変化させない

値：0 より始まり 0 x F F F F F F F F まで

【 0 1 4 6 】

BLOCK-SEED (8 バイト)

意味：1 ブロックを暗号化するための 1 つの鍵

機能：ブロックの先頭は、記録機器のセキュリティブロックで乱数を生成、続くブロックは、+ 1 インクリメントされた値、この値が失われると、1 ブロックに相当する約 1 秒間、音が出せないために、ヘッダとブロック末尾に同じものが二重に書かれる。編集されても値を変化させない

値：初期は 8 バイトの乱数

【 0 1 4 7 】

INITIALIZATION VECTOR (8 バイト)

意味：ブロック毎に A T R A C 3 データを暗号化、復号化する時に必要な初期値

機能：ブロックの先頭は 0 から始まり、次のブロックは最後の S U の最後の暗号化された 8 バイトの値。デバインドされたブロックの途中からの場合は開始 S U の直前の最後の 8 バイトを用いる。編集されても値を変化させない

値：0 から 0 x F F F F F F F F F F F F F F F F

【 0 1 4 8 】

S U - n n n

意味：サウンドユニットのデータ

機能：1.0 2 4 サンプルから圧縮されたデータ、圧縮モードにより出力されるバイト数が異なる。編集されても値を変化させない（一例として、S P モードの時では、N = 3 8 4 バイト）

値：A T R A C 3 のデータ値。

【 0 1 4 9 】

図 2 0 では、 $N = 384$ であるので、1 ブロックに 4 2 S U が書かれる。また、1 ブロックの先頭の 2 つのスロット (4 バイト) がヘッダとされ、最後の 1 スロット (2 バイト) に B L K I D - A 3 D、M C o d e、C O N N U M 0、B L O C K S E R I A L が二重に書かれる。従って、1 ブロックの余りの領域 M バイトは、 $(16, 384 - 384 \times 42 - 16 \times 3 = 208)$ (バイト) となる。この中に上述したように、8 バイトの B L O C K S E E D が二重に記録される。

【 0 1 5 0 】

ここで、フラッシュメモリ 3 4 に記憶されているデータは、後述するように例えば、A T R A C 3 方式で圧縮されている。圧縮の単位がサウンドユニット S U である。従って、記憶装置 3 0 0 から再生装置 2 0 0 にデータを読み出す場合には、読み出しの最小単位は当該サウンドユニット S U となる。オーディオデータの圧縮方式は、A T R A C 3 などの A T R A C 方式以外の C O D E C 方式でもよい。

【 0 1 5 1 】

ブロックシードデータ B S は、各ブロック毎に例えば乱数を発生して生成されたデータである。

【 0 1 5 2 】

〔フラッシュメモリ管理モジュール 3 5〕

フラッシュメモリ管理モジュール 3 5 は、フラッシュメモリ 3 4 へのデータの書き込み、フラッシュメモリ 3 4 からのデータの読み出しなどの制御を行う。

【 0 1 5 3 】

図 1 5 に示す再生装置 2 0 0 の構成について説明する。再生装置 2 0 0 は、例えば、主制御モジュール 4 1、通信インターフェイス 4 2、制御モジュール 4 3、編集モジュール 4 4、圧縮／伸長モジュール 4 5、スピーカ 4 6、D／A 変換器 4 7 および A／D 変換器 4 8 を有する。

【 0 1 5 4 】

〔主制御モジュール 4 1〕

主制御モジュール 4 1 は、再生装置 2 0 0 の処理を統括的に制御する。

【 0 1 5 5 】

〔制御モジュール 4 3〕

図 1 5 に示すように、制御モジュール 4 3 は、例えば、乱数発生ユニット 6 0、記憶ユニット 6 1、鍵生成／鍵演算ユニット 6 2、相互認証ユニット 6 3、暗号化／復号ユニット 6 4 および制御ユニット 6 5 を有する。制御モジュール 4 3 は、制御モジュール 3 3 と同様に、シングルチップの暗号処理専用の集積回路であり、多層構造を有し、内部のメモリセルはアルミニウム層などのダミー層に挟まれている。また、制御モジュール 4 3 は、動作電圧または動作周波数の幅が狭く、外部から不正にデータを読み出せないように耐タンパー性を有している。乱数発生ユニット 6 0 は、乱数発生指示を受けると、6 4 ビット（8 バイト）の乱数を発生する。記憶ユニット 6 1 は、認証処理に必要な種々のデータを記憶している。

【 0 1 5 6 】

鍵生成／鍵演算ユニット 6 2 は、例えば、ISO／IEC 9 7 9 7 の MAC 演算方式を用いた演算などの種々の演算を行って鍵データを生成する。このとき、“Block cipher Algorithm”として FIPS PUB 4 6 - 2 に規定される DES が用いられる。

【 0 1 5 7 】

相互認証ユニット 6 3 は、例えば、コンピュータから入力したオーディオデータを記憶装置 3 0 0 に出力する動作を行うのに先立って、記憶装置 3 0 0 との間で相互認証処理を行う。また、相互認証ユニット 6 3 は、記憶装置 3 0 0 からオーディオデータを入力する動作を行うのに先立って、記憶装置 3 0 0 との間で相互認証処理を行う。また、相互認証ユニット 6 3 は、相互認証処理において、前述した MAC 演算を行う。当該相互認証処理では、記憶ユニット 6 1 に記憶されているデータが用いられる。なお、相互認証ユニット 6 3 は、必要に応じて、例えば、パーソナルコンピュータ（PC）1 0 0 あるいはネットワーク上のコンピュータとの間でオーディオデータの入出力を行う動作に先立って、パーソナルコンピュータ（PC）1 0 0 あるいはネットワーク上のコンピュータとの間で相互認証処理を行う。

【 0 1 5 8 】

暗号化／復号ユニット 6 4 は、前述したように、F I P S P U B 8 1 に規定された E C B モードおよび C B C モードを選択的に用いてブロック暗号化を行う。

【 0 1 5 9 】

暗号化／復号ユニット 6 4 は、F I P S 8 1 のモードのうち、E C B モードおよび C B C モードの復号を選択的に行う。ここで、暗号化／復号ユニット 6 4 は、C B C モードにおいて、例えば 5 6 ビットの鍵データ k を用いて、暗号文を、6 4 ビットからなる暗号化ブロックを単位として復号して平文を生成する。

【 0 1 6 0 】

制御ユニット 6 5 は、乱数発生ユニット 6 0、記憶ユニット 6 1、鍵生成／鍵演算ユニット 6 2、相互認証ユニット 6 3 および暗号化／復号ユニット 6 4 の処理を統括的に制御する。

【 0 1 6 1 】

〔編集モジュール 4 4〕

編集モジュール 4 4 は、例えば、図 1 6 に示すように記憶装置 3 0 0 のフラッシュメモリ 3 4 内に記憶されたトラックデータファイルを、ユーザからの操作指示に基づいて編集して新たなトラックデータファイルを生成する。

【 0 1 6 2 】

〔圧縮／伸長モジュール 4 5〕

圧縮／伸長モジュール 4 5 は、例えば、記憶装置 3 0 0 から入力した暗号化されたオーディオデータを復号した後に再生する際に、A T R A C 3 方式で圧縮されているオーディオデータを伸長し、当該伸長したオーディオデータを D / A 変換器 4 7 に出力する。また、例えば、C D、D V D あるいは P C 1 から入力したオーディオデータを、記憶装置 3 0 0 に記憶する際に、当該オーディオデータを A T R A C 3 方式で圧縮する。

【 0 1 6 3 】

〔D / A 変換器 4 7〕

D / A 変換器 4 7 は、圧縮／伸長モジュール 4 5 から入力したデジタル形式の

オーディオデータをアナログ形式のオーディオデータに変換してスピーカ 4 6 に出力する。

【0 1 6 4】

〔スピーカ 4 6〕

スピーカ 4 6 は、D/A 変換器 4 7 から入力したオーディオデータに応じた音響を出力する。

【0 1 6 5】

〔A/D 変換器 4 8〕

A/D 変換器 4 8 は、例えば、CD プレーヤ 7 から入力したアナログ形式のオーディオデータをデジタル形式に変換して圧縮／伸長モジュール 4 5 に出力する。

【0 1 6 6】

〔コンテンツデータの記憶装置に対する格納処理および再生処理〕

図 1 5 に示す再生装置 2 0 0 と、記憶装置 3 0 0 との間では、コンテンツデータの移動、すなわち、再生装置 2 0 0 から記憶装置 3 0 0 のフラッシュメモリ 3 4 に対するデータ記録処理が実行され、さらに、記憶装置 3 0 0 のフラッシュメモリ 3 4 から再生装置 2 0 0 に対するデータ再生処理が実行される。

【0 1 6 7】

このデータ記録および再生処理について、以下説明する。まず、再生装置 2 0 0 から記憶装置 3 0 0 のフラッシュメモリ 3 4 に対するデータ記録処理を図 2 7 のフローを用いて説明する。

【0 1 6 8】

再生装置および記憶装置は、データ移動に先立ち、まずステップ S 2 7 0 1、S 2 7 0 2 に示す相互認証処理を実行する。図 2 8 に、共通鍵暗号方式を用いた相互認証方法 (ISO/IEC 9798-2) を示す。図 2 8 においては、共通鍵暗号方式として DES を用いているが、共通鍵暗号方式であれば他の方式も可能である。図 2 8 において、まず、B が 6 4 ビットの乱数 R b を生成し、R b および自己の ID である ID (b) を A に送信する。これを受信した A は、新たに 6 4 ビットの乱数 R a を生成し、R a、R b、ID (b) の順に、DES の CBC モードで鍵

K a b を用いてデータを暗号化し、B に返送する。なお、鍵 K a b は、A および B に共通の秘密鍵としてそれぞれの記録素子内に格納する鍵である。DES の CBC モードを用いた鍵 K a b による暗号化処理は、例えば DES を用いた処理においては、初期値と R a とを排他的論理和し、DES 暗号化部において、鍵 K a b を用いて暗号化し、暗号文 E 1 を生成し、続けて暗号文 E 1 と R b とを排他的論理和し、DES 暗号化部において、鍵 K a b を用いて暗号化し、暗号文 E 2 を生成し、さらに、暗号文 E 2 と I D (b) とを排他的論理和し、DES 暗号化部において、鍵 K a b を用いて暗号化して生成した暗号文 E 3 とによって送信データ (Token-AB) を生成する。

【 0 1 6 9 】

これを受信した B は、受信データを、やはり共通の秘密鍵としてそれぞれの記録素子内に格納する鍵 K a b (認証キー) で復号化する。受信データの復号化方法は、まず、暗号文 E 1 を認証キー K a b で復号化し、乱数 R a を得る。次に、暗号文 E 2 を認証キー K a b で復号化し、その結果と E 1 を排他的論理和し、R b を得る。最後に、暗号文 E 3 を認証キー K a b で復号化し、その結果と E 2 を排他的論理和し、I D (b) を得る。こうして得られた R a 、R b 、I D (b) のうち、R b および I D (b) が、B が送信したものと一致するか検証する。この検証に通った場合、B は A を正当なものとして認証する。

【 0 1 7 0 】

次に B は、認証後に使用するセッションキー (K s e s) を生成する (生成方法は、乱数を用いる)。そして、R b 、R a 、K s e s の順に、DES の CBC モードで認証キー K a b を用いて暗号化し、A に返送する。

【 0 1 7 1 】

これを受信した A は、受信データを認証キー K a b で復号化する。受信データの復号化方法は、B の復号化処理と同様であるので、ここでは詳細を省略する。こうして得られた R b 、R a 、K s e s の内、R b および R a が、A が送信したものと一致するか検証する。この検証に通った場合、A は B を正当なものとして認証する。互いに相手を認証した後には、セッションキー K s e s は、認証後の秘密通信のための共通鍵として利用される。

【0172】

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を終了（S2703でNo）する。

【0173】

相互認証が成立（S2703でYes）した場合は、ステップS2704において、再生装置がコンテンツキーKconの生成処理を実行する。この処理は、図15の乱数生成ユニット60で生成した乱数を用いて鍵生成／鍵演算ユニット62において実行される。

【0174】

次に、ステップS2705において、（1）コンテンツキーKconを有効化キープブロック（EKB）から取得される暗号化キーKEKを用いて暗号化処理して、E（KEK, Kcon）を生成するとともに、（2）コンテンツキーKconを認証処理において生成したセッションキー（Kses）で暗号化処理を実行して、E（Kses, Kcon）を生成して、記憶装置（メモリカード）に送信する。

【0175】

ステップS2706では、記憶装置が再生装置から受信したE（Kses, Kcon）をセッションキーで復号してコンテンツキーKconを取得し、さらに、Kconを記憶装置に予め格納されているストレージキーKstrによって暗号化してE（Kstr, Kcon）を生成し、これを再生装置に送信する。

【0176】

次に、再生装置は、ステップS2707において、ステップS2705で生成したE（KEK, Kcon）、およびステップS2706で記憶装置から受信したE（Kstr, Kcon）を用いて、データファイル（図20参照）を構成するトラック情報領域TRKINFデータを生成し、データファイルのフォーマット処理の後、これを記憶装置（メモリカード）に送信する。

【0177】

ステップS2708において、記憶装置（メモリカード）は、再生装置から受信したデータファイルをフラッシュメモリに格納する。

【0178】

このような処理により、データファイルのトラック情報領域TRKINFデータには、先に説明した図20、図22に示すように、コンテンツキーKconを有効化キーブロック(EKB)から取得される暗号化キーKEKを用いて暗号化処理したE(KEK, Kcon)と、コンテンツキーKconを記憶装置に予め格納されているストレージキーKstrによって暗号化したE(Kstr, Kcon)の2つの暗号化コンテンツキーが格納されることになる。

【0179】

なお、音楽データ、画像データ等の暗号化処理は、コンテンツキーKconをそのままコンテンツの暗号化鍵として適用して実行するか、あるいはコンテンツを構成するパーツ、またはブロック等を単位として、コンテンツキーと他のキー生成データに基づいて各パーツ単位、またはブロック単位の暗号化鍵を個別に生成して各パーツ単位、またはブロック単位の暗号化処理を行なう構成とすることが可能である。

【0180】

このようなデータファイルを用いた再生処理においては、再生装置は、E(KEK, Kcon)と、E(Kstr, Kcon)のいずれかを選択的に適用してコンテンツキーKconを取得可能となる。

【0181】

次に、再生装置200が記憶装置300のフラッシュメモリ34に格納されたデータの読み出し処理、すなわち再生処理を実行する場合の処理を図29のフローを用いて説明する。

【0182】

再生装置および記憶装置は、データ移動に先立ち、まずステップS2901、S2902に示す相互認証処理を実行する。この処理は、先に説明した図28の処理と同様である。相互認証が失敗した場合(S2903でNo)は、処理を終了する。

【0183】

相互認証が成立(S2903でYes)した場合は、ステップS2904にお

いて、記憶装置が再生装置に対してデータファイルを送信する。データファイルを受信した再生装置は、データファイル中のトラック情報領域TRKINFデータを検査し、コンテンツキー(Kcon)の格納状況を判別する。この判別処理は、キー有効化ブロック(EKB)によって取得される暗号化キーKEKによって暗号化されたコンテンツキー、すなわちE(KEK, Kcon)が格納されているか否かを判別する処理である。E(KEK, Kcon)の有無は、先の図20, 22で説明したデータファイル中のトラック情報領域TRKINFデータの[EKI]のデータにより判別可能である。

【0184】

E(KEK, Kcon)が格納されている場合(ステップS2906でYes)は、ステップS2907に進み、キー有効化ブロック(EKB)の処理により、暗号化キーKEKを取得して、取得した暗号化キーKEKにより、E(KEK, Kcon)を復号して、コンテンツキーKconを取得する。

【0185】

E(KEK, Kcon)が格納されていない場合(ステップS2906でNo)は、ステップS2908において、記憶装置の制御モジュール33において、記憶装置に予め格納されているストレージキーKstrによって暗号化したE(Kstr, Kcon)をストレージキーKstrによって復号して、さらに、相互認証処理において再生装置および記憶装置で共有したセッションキーKsesで暗号化したデータE(Kses, Kcon)を生成して、再生装置に送信する。

【0186】

再生装置は、ステップS2909において、記憶装置から受信したE(Kses, Kcon)をセッションキーKsesで復号してコンテンツキーKconを取得する。

【0187】

ステップS2910では、ステップS2907、またはステップS2909のいずれかにおいて取得したコンテンツキーKconにより暗号化コンテンツの復号を行なう。

【0188】

このように、暗号化コンテンツの再生処理において、再生装置は、 $E(K_{EK}, K_{con})$ を有効化キーブロック(EKB)から取得される暗号化キー K_{EK} を用いて復号するか、または、記憶装置に予め格納されているストレージキー K_{str} によって暗号化した $E(K_{str}, K_{con})$ に基づく処理を実行するか、いずれかの処理を実行することによりコンテンツキー K_{con} を取得することができる。

【0189】

なお、音楽データ、画像データ等の復号処理は、コンテンツキー K_{con} をそのままコンテンツの復号鍵として適用して実行するか、あるいはコンテンツを構成するパーツ、またはブロック等を単位として、コンテンツキーと他のキー生成データに基づいて各パーツ単位、またはブロック単位の復号鍵を個別に生成して各パーツ単位、またはブロック単位の復号処理を行なう構成とすることが可能である。

【0190】

[K_{EK} を格納したEKBのフォーマット]

先に図6を用いて有効化キーブロック(EKB)の概略的なフォーマットについて説明したが、さらに、キー暗号化キー(K_{EK})を有効化キーブロック(EKB)に格納して保持する場合の具体的なデータ構成例について説明する。

【0191】

図30にキー暗号化キー(K_{EK})を有効化キーブロック(EKB)に格納したデータであるEKBである配信鍵許可情報ファイルの構成例を示す。デバイス(再生装置)は、このファイルから必要に応じてキー暗号化キー(K_{EK})を取り出して、 K_{EK} により $E(K_{EK}, K_{con})$ を復号してコンテンツキー: K_{con} を取得してコンテンツの復号を実行する。各データについて説明する。

【0192】

BLKID-EKB (4バイト)

意味: BLOCKID FILE ID

機能: 配信鍵情報ファイルの先頭であることを識別するための値

値：固定値="EKB"（例えば0x454B4220）

【0193】

MC o d e（2バイト）

意味：MAKER CODE

機能：記録した機器の、メーカー、モデルを識別するコード

値：上位10ビット（メーカーコード） 下位6ビット（機種コード）

【0194】

L K F

意味：LINK FILE INFORMATION

機能：このEKBによって取得されるKEKが適用可能なコンテンツデータであるリンクファイルを識別する。

値：0～0xFF

bit 7：再生管理ファイル（PBLIST）に使用：1、未使用：0

bit 6：改竄チェック値（ICV）に使用：1、未使用：0

bit 5～0：リザーブ

【0195】

L I N K c o u n t

意味：LINK COUNT

機能：リンクしているファイル（例えばATRACK3ファイル）数

値：0～0xFFFFFFFF

【0196】

V e r s i o n

意味：VERSION

機能：配信鍵許可情報ファイルのバージョンを示す。

値：0～0xFFFFFFFF

【0197】

E A

意味：Encryption Algorithm

機能：配信鍵許可情報ファイルのトレース処理アルゴリズムを示す。

値：0～0xFF

00h：3DES：トリプルDESモードによる処理

01h：DES：シングルDESモードによる処理

なお、トリプルDESモードによる処理は、2種類以上の暗号処理キーを用いる暗号処理であり、シングルDESモードは1つのキーによる処理である。

【0198】

KEK1

意味：Key Encrypting Key

機能：キー有効化ブロック（EKB）中のルートキー（最上位）キーで暗号化されたコンテンツキー暗号キー

値：0～0xFFFFFFFFFFFFFFFF

【0199】

KEK2

意味：Key Encrypting Key

機能：キー有効化ブロック（EKB）中のルートキー（最上位）キーで暗号化されたコンテンツキー暗号キー

値：0～0xFFFFFFFFFFFFFFFF

【0200】

E (Version)

意味：Encrypted Version

機能：キー有効化ブロック（EKB）中のルートキー（最上位）キーで暗号化されたバージョン番号。復号時の下4バイトはリザーブ

値：0～0xFFFFFFFFFFFFFFFF

【0201】

Size of tag part

意味：Size of tag part

機能：配信鍵許可情報ファイルを構成するデータのタグ部分のサイズ（Byte）

値：0～0xFFFFFFFF

【0202】

Size of Key part

意味: Size of key part

機能: 配信鍵許可情報ファイルを構成するデータのキー部分のサイズ (Byte)

値: 0~0xFFFFFFFF

【0203】

Size of Sign part

意味: Size of sign part

機能: 配信鍵許可情報ファイルを構成するデータのサイン部分のサイズ (Byte)

値: 0~0xFFFFFFFF

【0204】

Tag part

意味: Tag part

機能: 配信鍵許可情報ファイルを構成するデータのタグ部分のデータ

値: すべての値

8バイトに満たない場合は0で埋めて8バイトにする。

【0205】

Key part

意味: Key part

機能: 配信鍵許可情報ファイルを構成するデータのキー部分のデータ

値: すべての値

【0206】

Signature part

意味: Signature part

機能: 配信鍵許可情報ファイルを構成するデータの署名 (Signature) 部分のデータ

値: すべての値

【 0 2 0 7 】

上述の説明および図 3 0 によって示されるように、デバイスに対して提供される配信鍵許可情報ファイルには、その配信鍵許可情報ファイルから取得される K E K が適用可能なコンテンツデータであるリンクファイルを識別するための識別データ [L K F] が格納され、さらに、リンクしているファイル（例えば A T R A C K 3 ファイル）数としてのデータ [L i n c C o u n t] が格納される。再生装置は、[L K F]、[L i n k C o u n t] を参照することにより、その配信鍵許可情報ファイルから取得される K E K を適用すべきデータが存在するか否かおよびその数を知ることが可能となる。

【 0 2 0 8 】

[リンク情報を用いたデータ復号、再生処理]

上述した配信鍵許可情報ファイルに含まれるリンクファイルを識別するための識別データ [L K F]、リンクしているファイル（例えば A T R A C K 3 ファイル）数としてのデータ [L i n c C o u n t] を用いて、効率的にデータの復号、再生を実行する処理態様について、以下説明する。

【 0 2 0 9 】

図 3 1 に記憶装置のデータ格納領域、例えば図 1 5 に示す記憶装置 3 0 0 のフラッシュメモリ 3 4 に格納されたデータファイル構成例を示す。ここでは、音楽データ（H I F I）のディレクトリ構成のみを例として示しているが、さらに、画像ファイル等のディレクトリが存在してもよい。

【 0 2 1 0 】

図 3 1 に示す音楽データのディレクトリには、再生管理ファイル（P B L I S T）、暗号化コンテンツとして複数の A T R A C K 3 データファイル（A 3 D）が含まれる。さらに、記憶装置には、複数の有効化キープブロックファイル（E K B n）が格納される。A T R A C K 3 データファイル（A 3 D）の復号処理に適用するコンテンツキーを取得するための有効化キープブロックファイル（E K B n）は、A T R A C K 3 データファイル（A 3 D）に含まれるポインタによって判別される。図 3 1 に示すように、1 つの有効化キープブロックファイル（E K B 1）3 1 0 1 は複数（3）の A T R A C K 3 データファイル（A 3 D）の復号処理に

適用される。

【0211】

この場合、有効化キープロックファイル（EKB1）3101に対応する配信鍵許可情報ファイルの[Linc Count]には3つのコンテンツに適用されることを示すデータが格納されることになる。

【0212】

図31のような複数のコンテンツファイル、複数の有効化キープロックファイルを格納した記憶装置であるメモリカードからコンテンツを復号して、再生する場合の処理フローを図32に示す。

【0213】

図32の処理は、例えば記憶装置としてのメモリカードを再生装置にセットした際、あるいはメモリカードを装着した再生装置の電源をONした際に再生装置が実行する処理である。

【0214】

まず、ステップS3201において、再生装置は、各々のEKBファイルのトラック情報を読み取り、[Linc Count]をチェックする。さらに、[Linc Count]のカウント数が多いものから順に、予め定められた個数[n]のEKBファイルを選択する。個数[n]は、再生装置の所定メモリ領域、すなわちキー暗号化キー：KEKを格納保持する領域に格納可能な個数に相当する個数として設定される。

【0215】

次に、ステップS3202において、選択したEKBの処理により、複数[n]のキー暗号化キー：KEKを取得し、これらを再生装置の鍵格納領域として設定されたRAMの所定領域に格納する。

【0216】

次に、再生装置は、ステップS3203において、復号、再生するコンテンツを選択する。さらに、ステップS3204において、その選択コンテンツの復号に適用するKEKがRAMに格納されているか否かを判定し、Yesの場合は、ステップS3205に進み、その対応KEKに基づいて、E(KEK, Kcon

) を復号してコンテンツキーを取得して、ステップ S 3 2 0 9 で再生、すなわち、取得したコンテンツキーによるデータの復号、再生処理を実行する。

【 0 2 1 7 】

ステップ S 3 2 0 4 において、選択コンテンツの復号に適用する K E K が R A M に格納されていない場合は、ステップ S 3 2 0 6 において、ストレージキーで暗号化されたコンテンツキー、すなわち、 $E(K_{str}, K_{con})$ の有無を判定し、ある場合は、ステップ S 3 2 0 7 において、 $E(K_{str}, K_{con})$ の復号処理によりコンテンツキーを取得して、ステップ S 3 2 0 9 で再生、すなわち、取得したコンテンツキーによるデータの復号、再生処理を実行する。

【 0 2 1 8 】

また、ステップ S 3 2 0 6 において、 $E(K_{str}, K_{con})$ がないと判定されると、その復号対象コンテンツに適用すべき E K B を記憶装置から取得して、取得した E K B の復号処理により K E K を取得し、取得した K E K による $E(K_{EK}, K_{con})$ の復号処理を実行してコンテンツキーを取得して、ステップ S 3 2 0 9 で再生、すなわち、取得したコンテンツキーによるデータの復号、再生処理を実行する。

【 0 2 1 9 】

このように、再生装置は、予め記憶装置に格納した複数のキー有効化ブロック (E K B) の [L i n e C o u n t] をチェックし、[L i n e C o u n t] のカウント数が多い E K B の復号を実行して、キー暗号化キー : K E K を格納しておく構成とすることにより、コンテンツ再生処理の際に、高い確率で R A M に格納した K E K を適用可能となり、効率的なコンテンツ再生が実行できる。

【 0 2 2 0 】

[キー有効化ブロック (E K B) による認証キー配信]

上述の有効化キーブロック (E K B) を使用したキーの配信において、認証処理を実行する際に使用する認証キー I K n を配信することにより、安全な秘密鍵として共有する認証キーを提供し、共通鍵方式に従った認証処理を実行する構成について説明する。

【 0 2 2 1 】

共通鍵暗号方式を用いた相互認証方法 (ISO/IEC 9798-2) は、先に図 2 8 を用いて説明した処理であり、データ送受信が実行される前の処理として、双方の正当性を確認するための処理として実行される。認証処理においては、データの送受信を行なう、例えば再生装置と記憶装置は認証キー K_{ab} を共有する。この共通鍵 K_{ab} を上述の有効化キープロック (EKB) を使用して再生装置に配信する。

【 0 2 2 2 】

図 3 3 および図 3 4 に複数のデバイスに共通の認証キー IK_n を有効化キープロック (EKB) によって配信する構成例を示す。図 3 3 はデバイス 0, 1, 2, 3 に対して復号可能な認証キー IK_n を配信する例、図 3 4 はデバイス 0, 1, 2, 3 中のデバイス 3 をリボーク (排除) してデバイス 0, 1, 2 に対してのみ復号可能な認証キーを配信する例を示す。

【 0 2 2 3 】

図 3 3 の例では、更新ノードキー $K(t)_{00}$ によって、認証キー IK_n を暗号化したデータ (b) とともに、デバイス 0, 1, 2, 3 においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキー $K(t)_{00}$ を復号可能な有効化キープロック (EKB) を生成して配信する。それぞれのデバイスは、図 3 3 の右側に示すようにまず、EKB を処理 (復号) することにより、更新されたノードキー $K(t)_{00}$ を取得し、次に、取得したノードキー $K(t)_{00}$ を用いて暗号化された認証キー: $Enc(K(t)_{00}, IK_n)$ を復号して認証キー IK_n を得ることが可能となる。

【 0 2 2 4 】

その他のデバイス 4, 5, 6, 7... は同一の有効化キープロック (EKB) を受信しても自身の保有するノードキー、リーフキーでは、EKB を処理して更新されたノードキー $K(t)_{00}$ を取得することができないので、安全に正当なデバイスに対してのみ認証キーを送付することができる。

【 0 2 2 5 】

一方、図 3 4 の例は、デバイス 3 が、例えば鍵の漏洩によりリボーク (排除) されているとして、他のグループのメンバ、すなわち、デバイス 0, 1, 2, に

対してのみ復号可能な有効化キープブロック (EKB) を生成して配信した例である。図 3 4 に示す (a) 有効化キープブロック (EKB) と、(b) 認証キー (IK_n) をノードキー (K(t) 00) で暗号化したデータを配信する。

【0226】

図 3 4 の右側には、復号手順を示してある。デバイス 0, 1, 2 は、まず、受領した有効化キープブロックから自身の保有するリーフキーまたはノードキーを用いた復号処理により、更新ノードキー (K(t) 00) を取得する。次に、K(t) 00 による復号により認証キー IK_n を取得する。

【0227】

他のグループのデバイス、例えばデバイス 4, 5, 6 … は、この同様のデータ (EKB) を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー (K(t) 00) を取得することができない。同様にリボークされたデバイス 3 においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー (K(t) 00) を取得することができず、正当な権利を有するデバイスのみが認証キーを復号して利用することが可能となる。

【0228】

このように、EKB を利用した認証キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした認証キーを配信することが可能となる。また、有効化キープブロック (EKB) によって暗号化され提供される EKB 配信認証鍵は、世代 (バージョン) 管理がなされ、世代毎の更新処理が実行され、任意のタイミングでのデバイスのリボーク (排除) が可能である。

【0229】

上述した EKB による認証キーの提供処理により、リボークされたデバイス (再生装置) では、記憶装置 (例えばメモリカード) との認証処理が成立せず、データの不正な復号が不可能となる。

【0230】

さらに、EKB を利用した認証キーの配送を用いれば、メモリカード以外の記憶媒体、例えば再生装置に内蔵したハードディスク等の記憶媒体に対するデータ格納、再生処理に対する制御も可能となる。

【 0 2 3 1 】

先の図 2 7 ～ 2 9 を用いて説明したように、記憶装置を利用したコンテンツの記録、再生処理においては、相互認証処理が実行され、相互認証処理の成立を条件として、データの記録および再生が可能となる。この認証処理プログラムは、メモリカードのような相互認証処理が可能な記憶装置との間での処理においては有効に作用するが、例えば、再生装置がハードディスク、CD-R 等、暗号処理機能を持たない、すなわち相互認証を実行不可能な記憶媒体に対してデータ格納、データ再生時には意味をなさないことになる。しかし、本発明のシステムでは、このような認証不可能な機器を利用したデータ格納、あるいはデータ再生処理においても認証処理プログラムを実行させる構成とする。ハードディスク、CD-R 等は相互認証が不可能であるので、仮想のメモリカード（メモリスティック）を再生装置に構成し、仮想メモリカードと再生装置間において認証処理を実行させて、認証成立を条件として、認証機能を持たない記憶媒体に対するデータ格納処理、あるいは記憶媒体からのデータ再生を可能とする。

【 0 2 3 2 】

これらの仮想メモリカードを使用したデータ記録、再生処理フローを図 3 5 に示す。まず、再生装置は、再生装置内の仮想メモリカードとの間で相互認証処理を実行する。ステップ S 3 5 0 2 において、認証成立したか否かを判定し、成立したことを条件としてステップ S 3 5 0 3 に進み、認証機能を持たない記憶媒体、例えばハードディスク、CD-R、DVD 等を用いたデータ記録、再生処理を実行する。

【 0 2 3 3 】

ステップ S 3 5 0 2 において、認証が成立しなかったと判定された場合は、ステップ S 3 5 0 3 の認証機能を持たない記憶媒体、例えばハードディスク、CD-R、DVD 等を用いたデータ記録、再生処理が実行されない。

【 0 2 3 4 】

ここで、仮想メモリカードには、予め、先の図 1 6 で説明した認証鍵データを格納した構成とし、再生装置が使用する認証キーを前述したように、キー有効化ブロックで提供する構成とする。

【 0 2 3 5 】

このように、再生装置の認証キーをキー有効化ブロック（E K B）で提供することにより、正当なライセンスを持つデバイス（再生装置）に対してのみ、仮想メモリカードとの相互認証可能な認証キーを配信することが可能となる。従って、不正な機器、すなわちリボークされた再生装置には、有効な認証キーが配信しない処理が可能となる。有効な認証キーが提供されない再生装置は、相互認証が不成立となり、認証機能を持つメモリカードのみならず、認証機能を持たない記憶媒体、例えばハードディスク、C D - R、D V D等を用いたデータ記録、再生処理が実行されず、不正な機器によるデータ記録、再生を排除することが可能となる。

【 0 2 3 6 】

すなわち、認証鍵を提供する有効化キーブロック（E K B）をキーツリーのリーフを構成するデータ処理装置中、正当なライセンスを持つデータ処理装置においてのみ復号可能で、正当ライセンスを持たない不正なデータ処理装置においては復号不可能な有効化キーブロック（E K B）として提供することにより、不正なデータ処理装置における仮想メモリデバイスとの認証成立を防止して、不正データ処理装置におけるコンテンツ利用を排除可能とした構成を有するライセンスシステムが実現される。

【 0 2 3 7 】

[チェック値（I C V: Integrity Check Value）格納構成]

次に、コンテンツの改竄を防止するためにコンテンツのインテグリティ・チェック値（I C V）を生成して、コンテンツに対応付けて、I C Vの計算により、コンテンツ改竄の有無を判定する処理構成について説明する。

【 0 2 3 8 】

コンテンツのインテグリティ・チェック値（I C V）は、例えばコンテンツに対するハッシュ関数を用いて計算され、 $I C V = \text{hash}(K i c v, C 1, C 2, \dots)$ によって計算される。K i c vはI C V生成キーである。C 1, C 2はコンテンツの情報であり、コンテンツの重要情報のメッセージ認証符号（M A C : Message authentication Code）が使用される。前述したように、[M A C]

は、図 2 0 で説明した A T R A C 3 データファイルにも含まれる。これらを使用してインテグリティ・チェック値 (I C V) の計算がなされる。

【 0 2 3 9 】

D E S 暗号処理構成を用いた M A C 値生成例を図 3 6 に示す。図 3 6 の構成に示すように対象となるメッセージを 8 バイト単位に分割し、(以下、分割されたメッセージを M 1、M 2、・・・、M N とする)、まず、初期値 (Initial Value (以下、I V とする)) と M 1 を排他的論理和する(その結果を I 1 とする)。次に、I 1 を D E S 暗号化部に入れ、鍵(以下、K 1 とする)を用いて暗号化する(出力を E 1 とする)。続けて、E 1 および M 2 を排他的論理和し、その出力 I 2 を D E S 暗号化部へ入れ、鍵 K 1 を用いて暗号化する(出力 E 2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきた E N がメッセージ認証符号 (M A C (Message Authentication Code)) となる。なお、メッセージとしては、検証対象となるコンテンツおよびヘッダ情報等のコンテンツ関連データを構成する部分データが使用可能である。

【 0 2 4 0 】

このようなコンテンツの M A C 値と I C V 生成キー K i c v にハッシュ関数を適用して用いてコンテンツのインテグリティ・チェック値 (I C V) が生成される。改竄のないことが保証された例えばコンテンツ生成時に生成した I C V と、新たにコンテンツに基づいて生成した I C V とを比較して同一の I C V が得られればコンテンツに改竄のないことが保証され、I C V が異なれば、改竄があったと判定される。

【 0 2 4 1 】

上述のようなインテグリティ・チェック値 (I C V) は、コンテンツ個々に対して生成される複数のコンテンツ M A C 値により、1 つのインテグリティ・チェック値 (I C V) を生成することが可能である。複数の M A C による I C V の計算は、例えば、 $I C V = M A C (K i c v, C_M A C [0] || C_M A C [1] || C_M A C [2] || \dots)$ によって生成する。

【 0 2 4 2 】

コンテンツ生成時に生成した I C V を格納しておき、チェック処理時に生成 I

ＣＶと格納ＩＣＶの比較処理を行なう。両ＩＣＶが一致すれば改竄無しと判定し、ＩＣＶが不一致の場合は、改竄が有りと判定され、データ再生等の処理制限がなされる。

【 0 2 4 3 】

メモリカード等の記憶装置には、音楽コンテンツのみならず、画像データ、ゲームプログラムデータ等、カテゴリの異なるが格納される。これら各カテゴリのコンテンツも改竄の防止を図るため、各カテゴリ毎にインテグリティ・チェック値（ＩＣＶ）を生成して格納することがコンテンツ改竄チェックのためには有効な手段となる。

【 0 2 4 4 】

しかしながら、メモリに格納するコンテンツ数が増大すると、検証用のチェック値を正規のコンテンツデータに基づいて生成し、格納し管理することが困難となる。特に、昨今フラッシュメモリを使用したメモリカード等の容量の大きい媒体においては、音楽データ、画像データ、プログラムデータ等、様々なカテゴリのコンテンツデータがメモリに格納されることとなる。このような環境においては、チェック値の生成処理、格納処理、改竄チェック処理の管理は困難となる。格納データ全体に対するチェック値を生成すると、チェック対象となったデータ全体に対するチェック値生成処理を実行することが必要となる。例えばDES-CBCモードにおいて生成されるメッセージ認証符号（MAC）により、チェック値ＩＣＶを求める手法を行なう場合、データ全体に対するDES-CBCの処理を実行することが必要となる。この計算量は、データ長が長くなるにつれ増大することとなり、処理効率の点で問題がある。

【 0 2 4 5 】

記憶装置として使用可能なメモリカードには、多くのカテゴリの異なるコンテンツが格納される。これらのカテゴリの異なるコンテンツの改竄チェック管理をカテゴリ毎に独立したインテグリティ・チェック値（ＩＣＶ）を生成して実行する構成とすることにより、ＩＣＶのチェック時、あるいはＩＣＶの変更時、例えばデータ変更時の新たなインテグリティ・チェック値（ＩＣＶ）の生成処理が、1つのカテゴリ内のデータを対象として実行可能となり、他のカテゴリに影響を

及ぼすことがない。このようにカテゴリ毎の複数のインテグリティ・チェック値（ICV）を格納する構成について説明する。

【0246】

図37に記憶装置に格納されるデータ構成と、それぞれのインテグリティ・チェック値（ICV）の格納構成例を示す。メモ리카ード等の記憶部（フラッシュメモリ）には、図37に示されるように音楽データのディレクトリに、再生管理ファイル（PBLIST）、暗号化コンテンツとして複数のATRACK3データファイル（A3D）が含まれ、さらに、メモリには、複数のカテゴリに属するコンテンツデータ（#1～#n）が格納される。複数のカテゴリとは、例えば、音楽データ、画像データ、ゲームプログラム等である。さらに、同様の画像データであっても、それぞれのデータ提供元に応じて別のディレクトリとして独立のカテゴリとして管理してもよい。

【0247】

また、前述の有効化キープブロック（EKB）の管理単位（エンティティ）を1カテゴリとして設定してもよい。すなわち、ある有効化キープブロック（EKB）によって取得されるキー暗号キー：KEKによって復号されるコンテンツキーKconを適用可能なコンテンツ集合を1つのカテゴリとして設定してもよい。

【0248】

再生管理ファイル（PBLIST）、暗号化コンテンツとして複数のATRACK3データファイル（A3D）の各々には、改竄チェックのためのメッセージ認証符号（MAC（Message Authentication Code））が含まれ、これらのMAC値に基づいてインテグリティ・チェック値（ICV（con））が生成される。複数のコンテンツのMAC値は、フラッシュメモリのシーケンスページにMACリストとして格納、管理され、これらのMACリストに基づいてICV生成キーKicvを適用して得られるインテグリティ・チェック値（ICV（con））が格納保存される。

【0249】

コンテンツMAC値を格納するシーケンスページフォーマットを図38に示す。シーケンスページ領域は、一般コンテンツデータの書き込み禁止領域として設

定された領域である。図38のシーケンスページ構成について説明する。

【0250】

E(kSTR, kCON)は、メモ리카ードのストレージキーで暗号化したコンテンツキーである。ID(upper), (lower)は、メモ리카ードの識別子(ID)の格納領域である。C_MAC[0]は、再生管理ファイル(PBLIST)の構成データに基づいて生成されたMAC値である。C_MAC[1]は、コンテンツ、例えばATRACK3データファイル#1のデータに基づいて生成されたMAC値、以下、コンテンツ毎にMAC値が格納される。これらのMAC値に基づいてインテグリティ・チェック値(ICV(con))が生成され、生成されたICV(con)がシリアルプロトコルを通してメモリに書き込まれる。なお、異なる鍵システムに対応するため、それぞれの鍵システムから生成されるICVをそれぞれ違うエリアに格納する構成とすることが好ましい。

【0251】

また、カテゴリ毎に改竄チェックのために生成される各カテゴリ毎のインテグリティ・チェック値(ICV)は、メモ리카ードの記憶部(フラッシュメモリ)のプールページに記録される。プールページもまた、一般データの書き込みの禁止された領域として設定されている。

【0252】

各カテゴリ毎のインテグリティ・チェック値(ICV)を格納するプールページフォーマットを図39に示す。#0__revisionは、カテゴリ#0の更新データが設定され、更新された場合はインクリメントされる。#0__versionは、カテゴリ#0のバージョン、#0__E(KEK, Kicv)は、カテゴリ#0のキー暗号化キー(KEK)で暗号化したICV生成キー(Kicv)であり、ICV0は、カテゴリ#0のインテグリティ・チェック値(ICV)値である。以下、同様のデータが各カテゴリ毎にEKB#15まで格納可能となっている。

【0253】

ICVのチェックは、パワーオン時、またはメモ리카ード等の記憶装置が再生装置にセットされたことを条件として開始される。図40にICVチェックを含

む処理フローを示す。

【0254】

まず、再生装置がパワーオン、または新たなメモリカード等が装着されたことを検知すると、ステップS4001において、再生装置と記憶装置間の相互認証が可能か否かが判定され、可能である場合は、ステップS4002において記憶装置と再生装置間での相互認証処理（図28参照）が実行される。また、ステップS4001において、再生装置と記憶装置間の相互認証が可能でないと判定された場合は、ステップS4003において、前述した仮想メモリカードと再生装置間の相互認証処理が実行される。

【0255】

ステップS4004で相互認証が成立したか否かが判定され、不成立の場合は、以下の処理は実行されないで終了する。相互認証が成立の場合は、ステップS4005においてICVの計算が実行される。ICVは、前述したように各ファイルのMAC値に基づいて算出される。

【0256】

次にステップS4006において、計算によって算出された生成ICVと、予め格納してある格納ICVとの比較が実行される。両ICVが一致した場合は、データ改竄がないと判定され、ステップS4007において、データ再生等の様々な処理が実行される。一方、ICVが不一致であった場合は、データ改竄があると判定され、データの再生等を行わず処理を終了する。このような処理を実行することによりデータ改竄の防止、改竄されたデータの再生が排除される。

【0257】

このように、カテゴリの異なるコンテンツについて、カテゴリ毎に独立したインテグリティ・チェック値（ICV）を生成して管理する構成とすることにより、ICVのチェック時、あるいはICVの変更時、例えばデータ変更時の新たなインテグリティ・チェック値（ICV）の生成処理が、1つのカテゴリ内のデータを対象として実行可能となり、他のカテゴリに影響を及ぼすことがない。

【0258】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしな

がら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【 0 2 5 9 】

【発明の効果】

以上、説明したように、本発明の情報処理装置、および方法によれば、記憶装置に格納されるコンテンツの検証値を生成してコンテンツに対応付けて格納し、コンテンツ改竄の有無を前記検証値により実行する構成において、検証値をコンテンツのカテゴリ毎に独立した検証値として生成して格納する構成としたので、コンテンツデータの検証処理の効率化、さらに検証後の記録デバイスに対するダウンロード処理、あるいは検証後の再生処理等を効率的に実行することが可能となる。

【 0 2 6 0 】

さらに、本発明の情報処理装置、および方法によれば、カテゴリは、コンテンツの種類、あるいは、コンテンツの暗号処理鍵として設定されるコンテンツキー K c o n を暗号化して提供する有効化キーブロック (E K B) の管理エンティティに基づいて設定された構成としたので、例えば有効化キーブロック (E K B) の管理エンティティ別に、コンテンツデータの検証処理を独立して実行可能となり、処理の効率化が実現される。

【図面の簡単な説明】

【図 1】

本発明の情報処理システムの使用概念を説明する図である。

【図 2】

本発明の情報処理システムのシステム構成例およびデータ経路例を示す図である。

【図 3】

本発明の情報処理システムにおける各種キー、データの暗号化処理について説明するツリー構成図である。

【図 4】

本発明の情報処理システムにおける各種キー、データの配布に使用される有効化キーブロック（E K B）の例を示す図である。

【図 5】

本発明の情報処理システムにおけるコンテンツキーの有効化キーブロック（E K B）を使用した配布例と復号処理例を示す図である。

【図 6】

本発明の情報処理システムにおける有効化キーブロック（E K B）のフォーマット例を示す図である。

【図 7】

本発明の情報処理システムにおける有効化キーブロック（E K B）のタグの構成を説明する図である。

【図 8】

本発明の情報処理システムにおける有効化キーブロック（E K B）と、コンテンツキー、コンテンツを併せて配信するデータ構成例を示す図である。

【図 9】

本発明の情報処理システムにおける有効化キーブロック（E K B）と、コンテンツキー、コンテンツを併せて配信した場合のデバイスでの処理例を示す図である。

【図 1 0】

本発明の情報処理システムにおける有効化キーブロック（E K B）とコンテンツを記録媒体に格納した場合の対応について説明する図である。

【図 1 1】

本発明の情報処理システムにおける階層ツリー構造のカテゴリ分類の例を説明する図である。

【図 1 2】

本発明の情報処理システムにおける簡略化有効化キーブロック（E K B）の生成過程を説明する図である。

【図 1 3】

本発明の情報処理システムにおける有効化キープブロック（E K B）の生成過程を説明する図である。

【図 1 4】

本発明の情報処理システムにおける簡略化有効化キープブロック（E K B）を説明する図である。

【図 1 5】

本発明の情報処理システムにおける再生装置と記憶装置の構成を示すブロック図である。

【図 1 6】

本発明の情報処理システムにおける記憶装置内の記憶ユニットに記憶されているデータを説明する図である。

【図 1 7】

本発明の情報処理システムにおける記憶装置のフラッシュメモリに記憶されるデータを説明するための図である。

【図 1 8】

本発明の情報処理システムにおける再生管理ファイルのデータ構成を概略的に示す図である。

【図 1 9】

本発明の情報処理システムにおけるデータファイルのデータ構成を概略的に示す図である。

【図 2 0】

本発明の情報処理システムにおけるデータファイルのデータ構成をより詳細に示す図である。

【図 2 1】

本発明の情報処理システムにおけるデータファイルの属性ヘッダの一部を示す図である。

【図 2 2】

本発明の情報処理システムにおけるデータファイルの属性ヘッダの一部を示す図である。

【図 2 3】

本発明の情報処理システムにおけるモードの種類と、各モードにおける録音時間等を示す図である。

【図 2 4】

本発明の情報処理システムにおけるコピー制御情報を説明するための図である。

【図 2 5】

本発明の情報処理システムにおけるデータファイルの属性ヘッダの一部を示す図である。

【図 2 6】

本発明の情報処理システムにおけるデータファイルの各データブロックのヘッダを示す略線図である。

【図 2 7】

本発明の情報処理システムにおけるデータ記録処理フローを示す図である。

【図 2 8】

本発明の情報処理システムにおいて適用可能な相互認証処理を示す図である。

【図 2 9】

本発明の情報処理システムにおけるデータ再生処理フローを示す図である。

【図 3 0】

本発明の情報処理システムにおける配信鍵許可情報ファイルのフォーマットを示す図である。

【図 3 1】

本発明の情報処理システムにおけるデータ格納態様を示す図である。

【図 3 2】

本発明の情報処理システムにおけるキー有効化ブロック（E K B）を使用したデータ復号処理フローを示す図である。

【図 3 3】

本発明の情報処理システムにおける有効化キーブロック（E K B）と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その 1）であ

る。

【図 3 4】

本発明の情報処理システムにおける有効化キープブロック（EKB）と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その2）である。

【図 3 5】

本発明の情報処理システムにおける仮想メモリカードを適用したて認証処理シーケンスを示す図である。

【図 3 6】

本発明の情報処理システムにおいて適用可能なインテグリティ・チェック値（ICV）の生成に使用するMAC値生成例を示す図である。

【図 3 7】

本発明の情報処理システムにおけるインテグリティ・チェック値（ICV）の格納態様を説明する図である。

【図 3 8】

本発明の情報処理システムにおけるMAC値を格納するシーケンスページフォーマットを示す図である。

【図 3 9】

本発明の情報処理システムにおけるICVを格納するプールページフォーマットを示す図である。

【図 4 0】

本発明の情報処理システムにおけるICVチェック処理フローを示す図である。

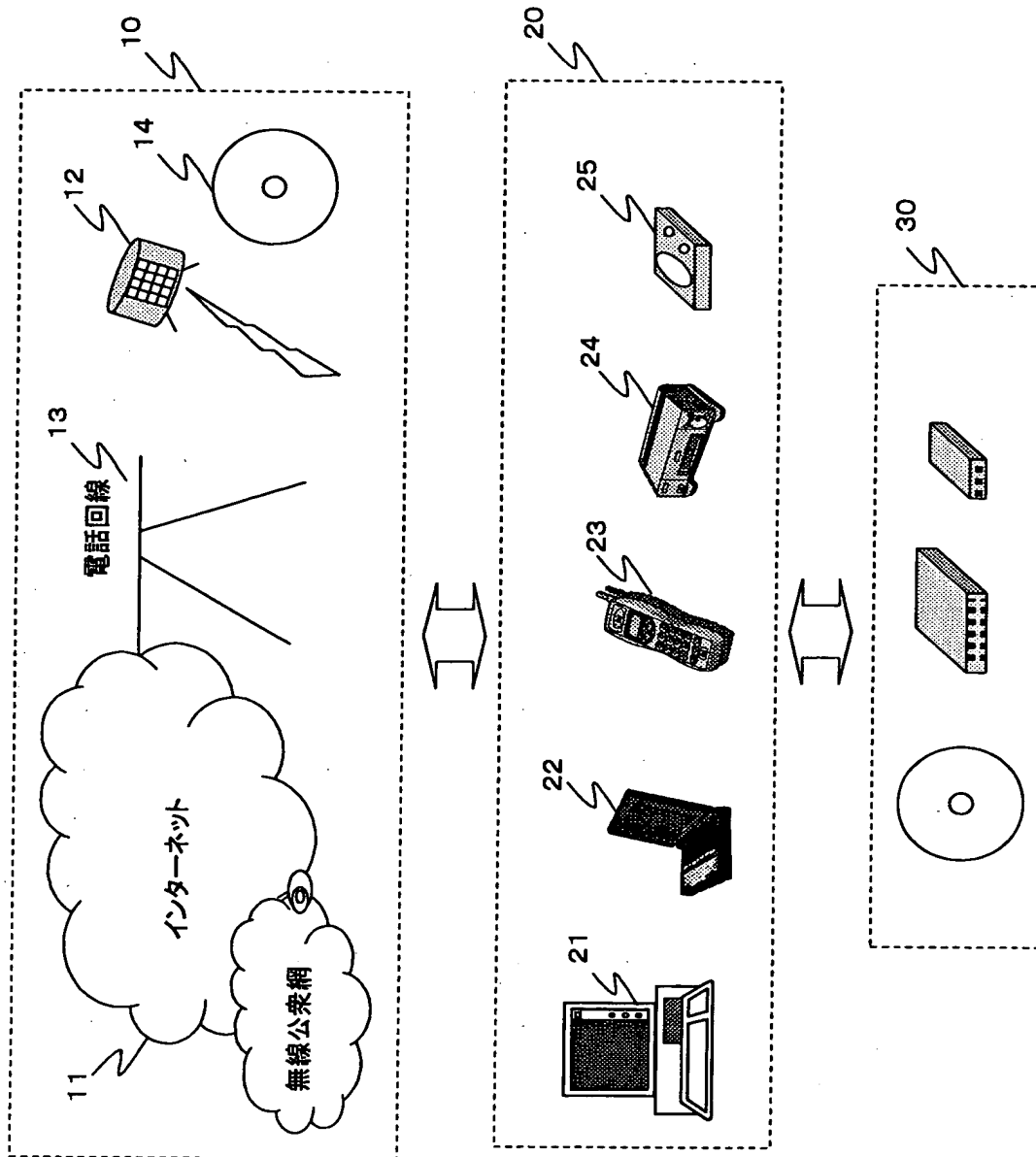
【符号の説明】

- 1 0 コンテンツ配信手段
- 1 1 インターネット
- 1 2 衛星放送
- 1 3 電話回線
- 1 4 メディア

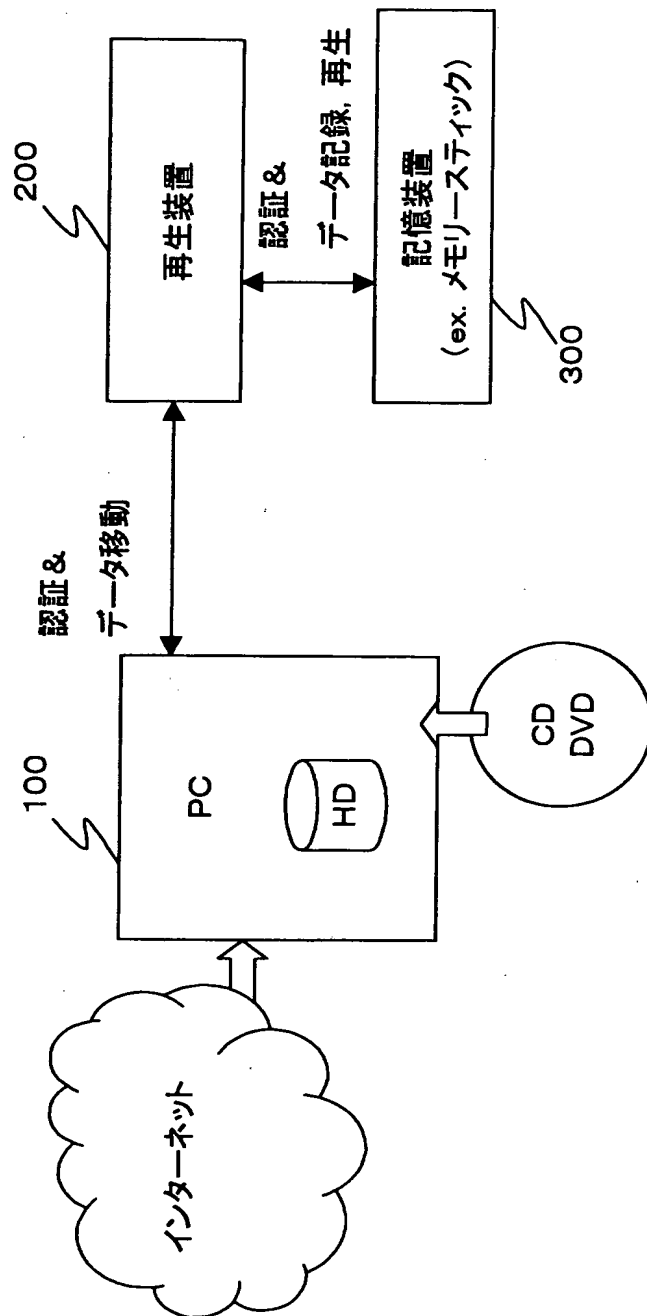
- 2 0 データ処理手段
- 2 1 パーソナルコンピュータ (P C)
- 2 2 ポータブルデバイス (P D)
- 2 3 携帯電話、P D A
- 2 4 記録再生器、ゲーム端末
- 2 5 再生装置
- 3 0 記憶手段
- 1 0 0 パーソナルコンピュータ (P C)
- 2 0 0 再生装置
- 3 0 0 記憶装置
- 6 0 1 バージョン
- 6 0 2 デプス
- 6 0 3 データポインタ
- 6 0 4 タグポインタ
- 6 0 5 署名ポインタ
- 6 0 6 データ部
- 6 0 7 タグ部
- 6 0 8 署名
- 3 3, 4 3 制御モジュール
- 5 0, 6 0 乱数発生ユニット
- 5 1, 6 1 記憶ユニット
- 5 2, 6 2 鍵生成／演算ユニット
- 5 3, 6 3 相互認証ユニット
- 5 4, 7 4 暗号化／復号ユニット
- 5 5, 6 5 制御ユニット
- 3 4 フラッシュメモリ
- 4 4 編集モジュール
- 4 5 圧縮／伸長モジュール
- 4 6 スピーカ

【書類名】 図面

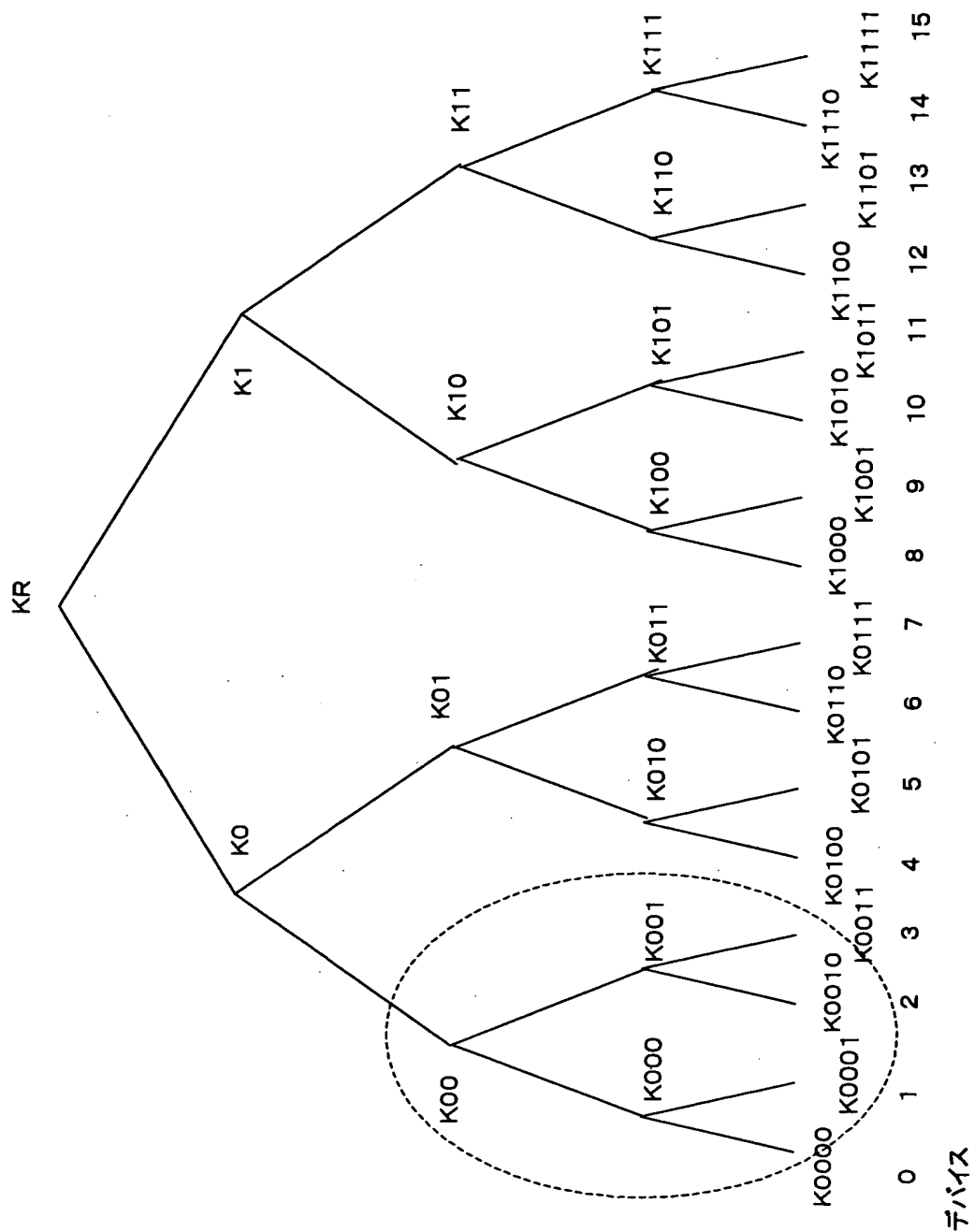
【図 1】



【図 2】



【図 3】



【図 4】

(A) 有効化キーブロック(EKB:Enabling Key Block) 例1

デバイス0, 1, 2にバージョン:tのノードキーを送付

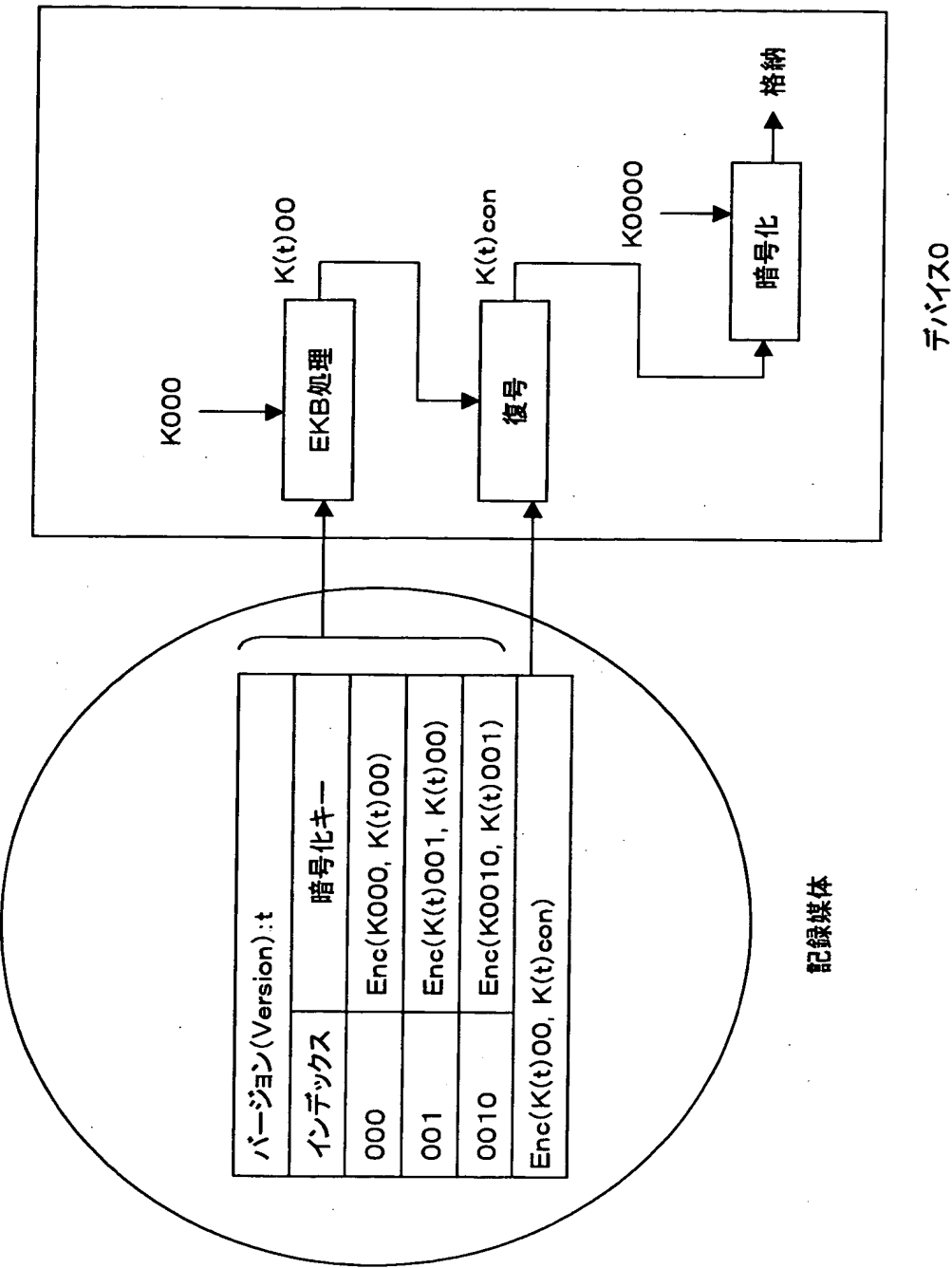
バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) 有効化キーブロック(EKB:Enabling Key Block) 例2

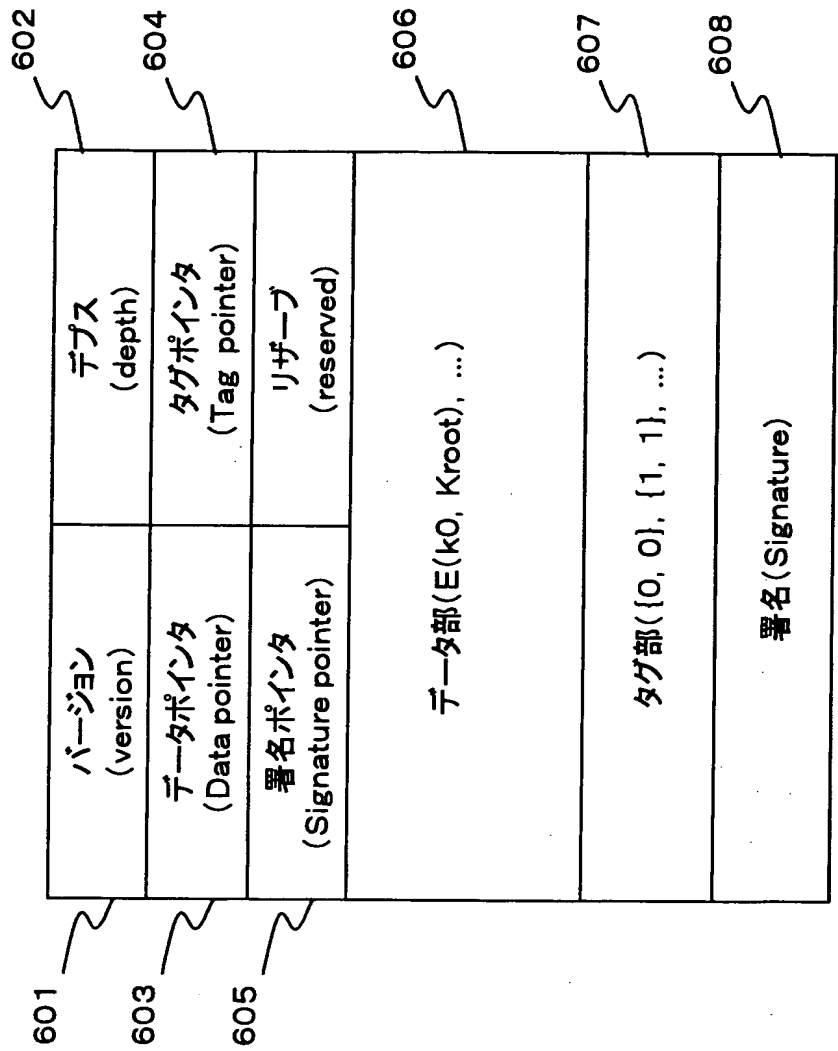
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

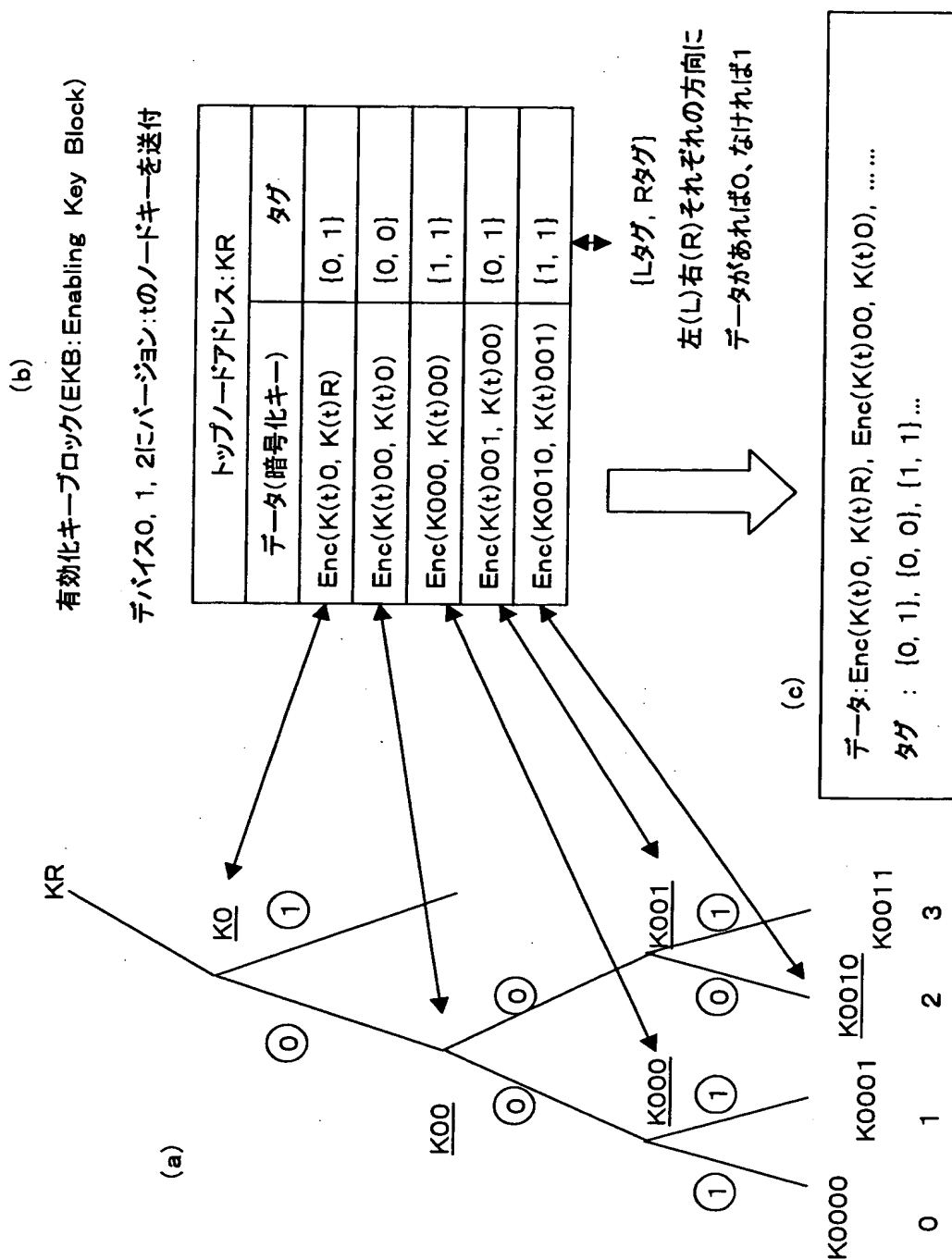
【図 5】



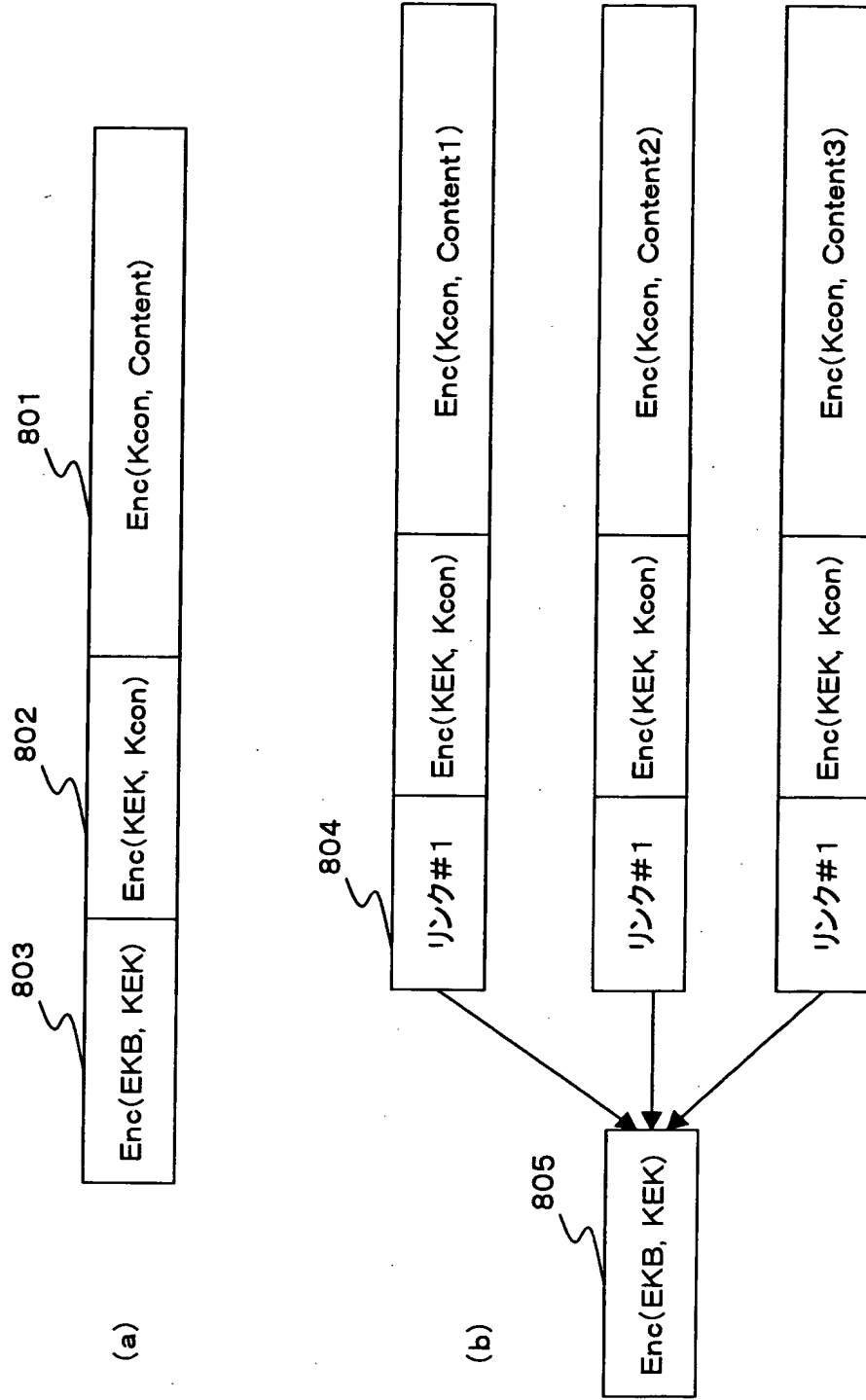
【図 6】



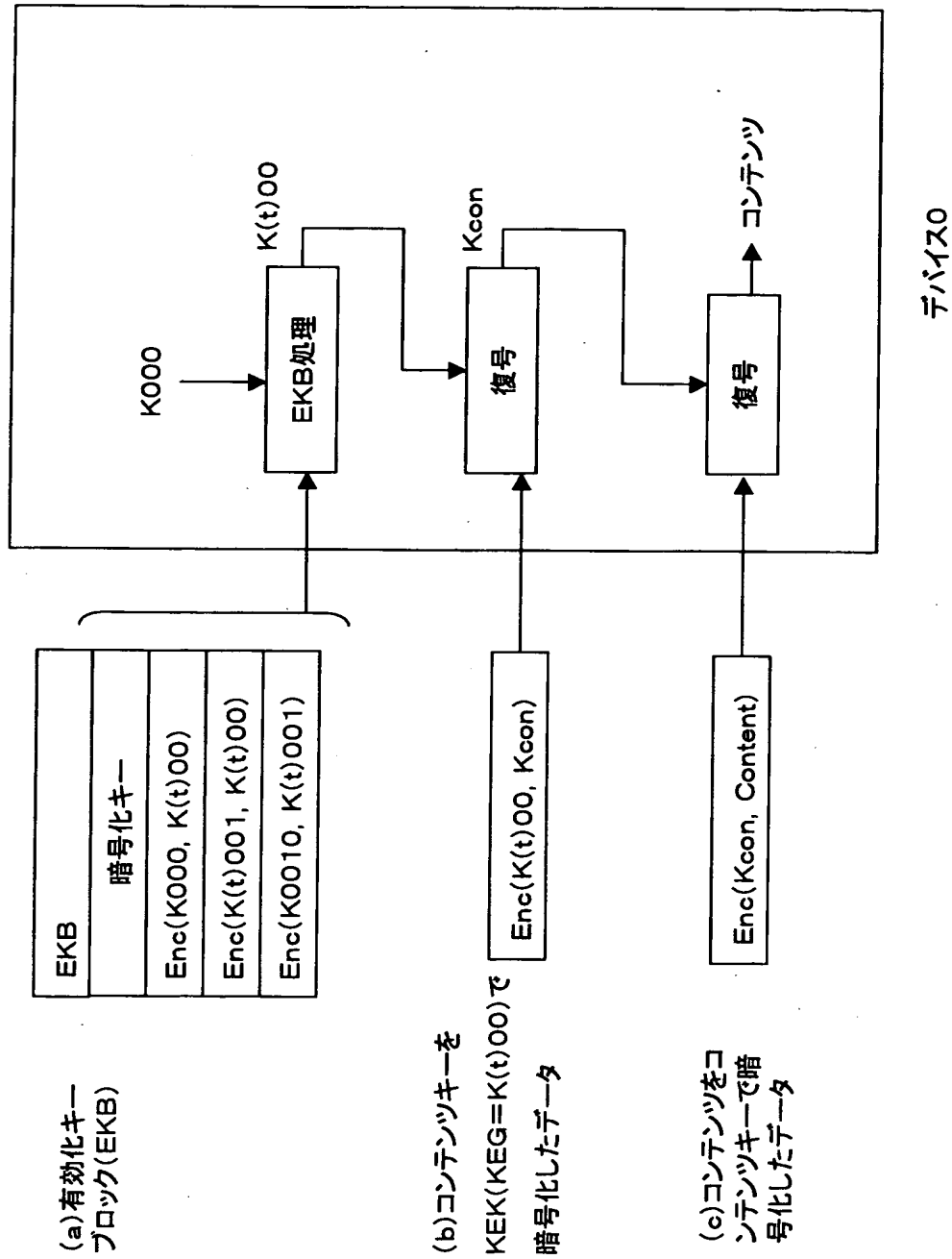
【図 7】



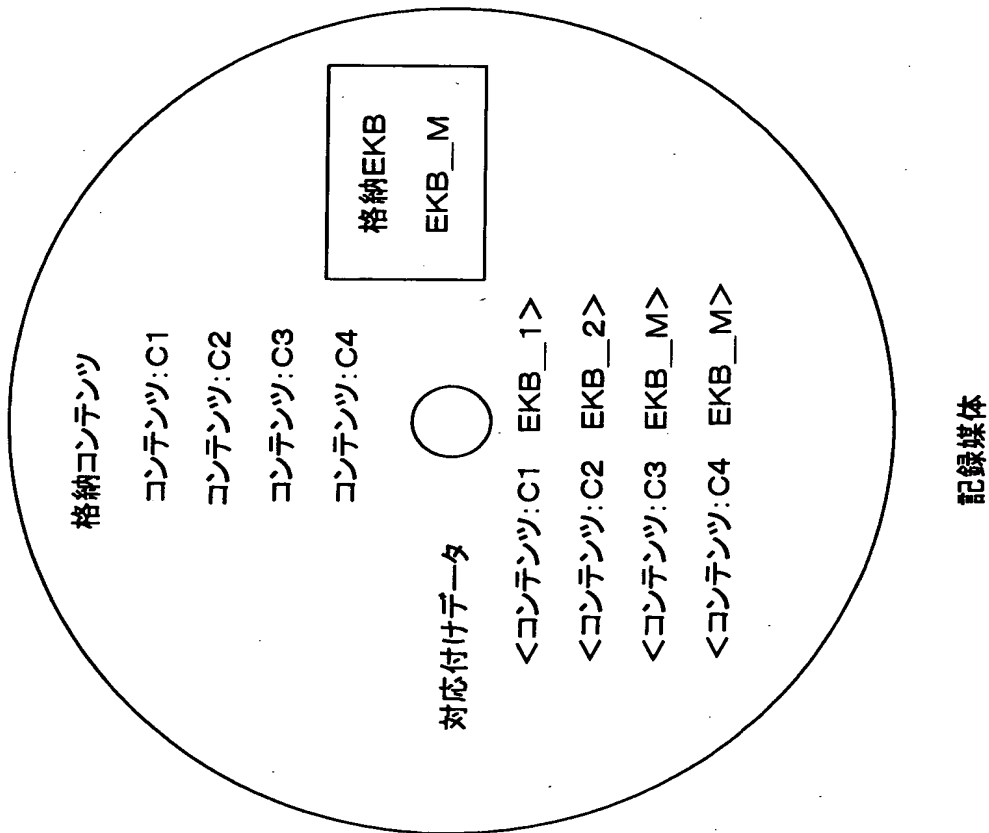
【図 8】



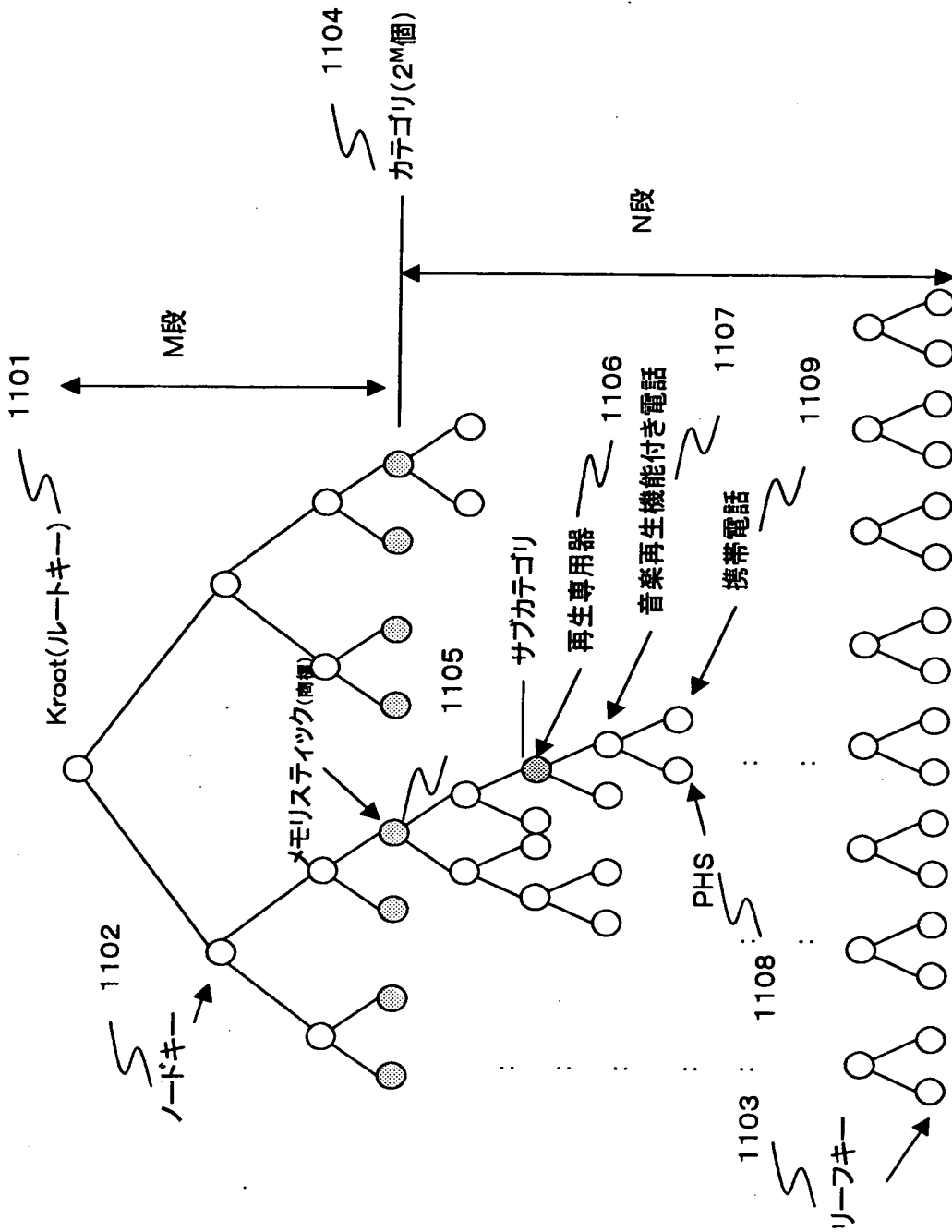
【図9】



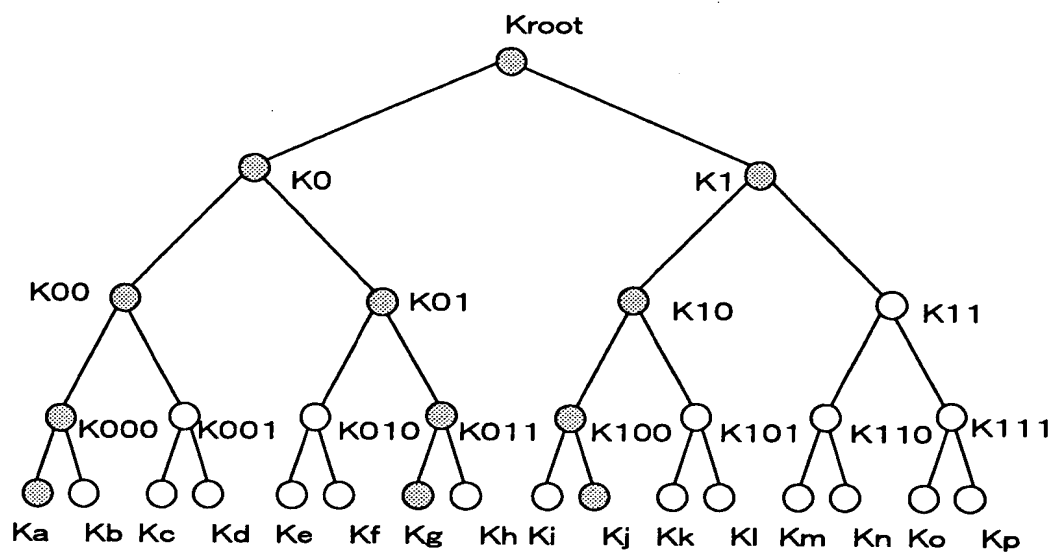
【図 1 0】



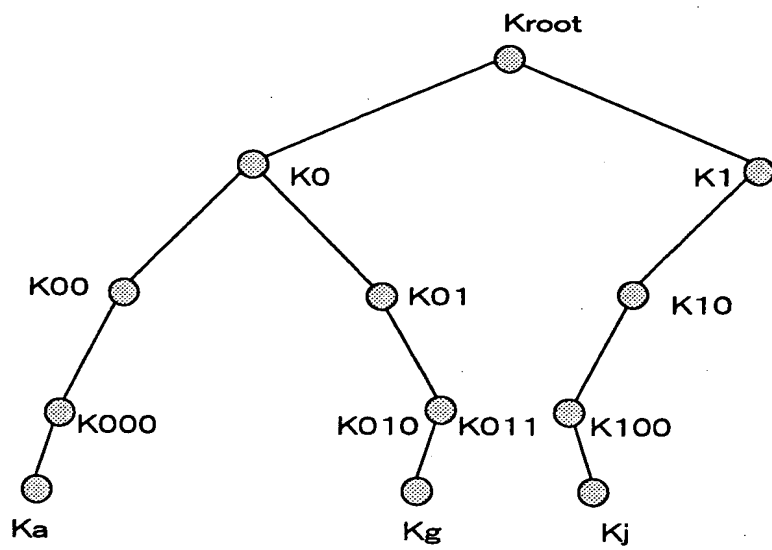
【図 11】



【図 1 2】



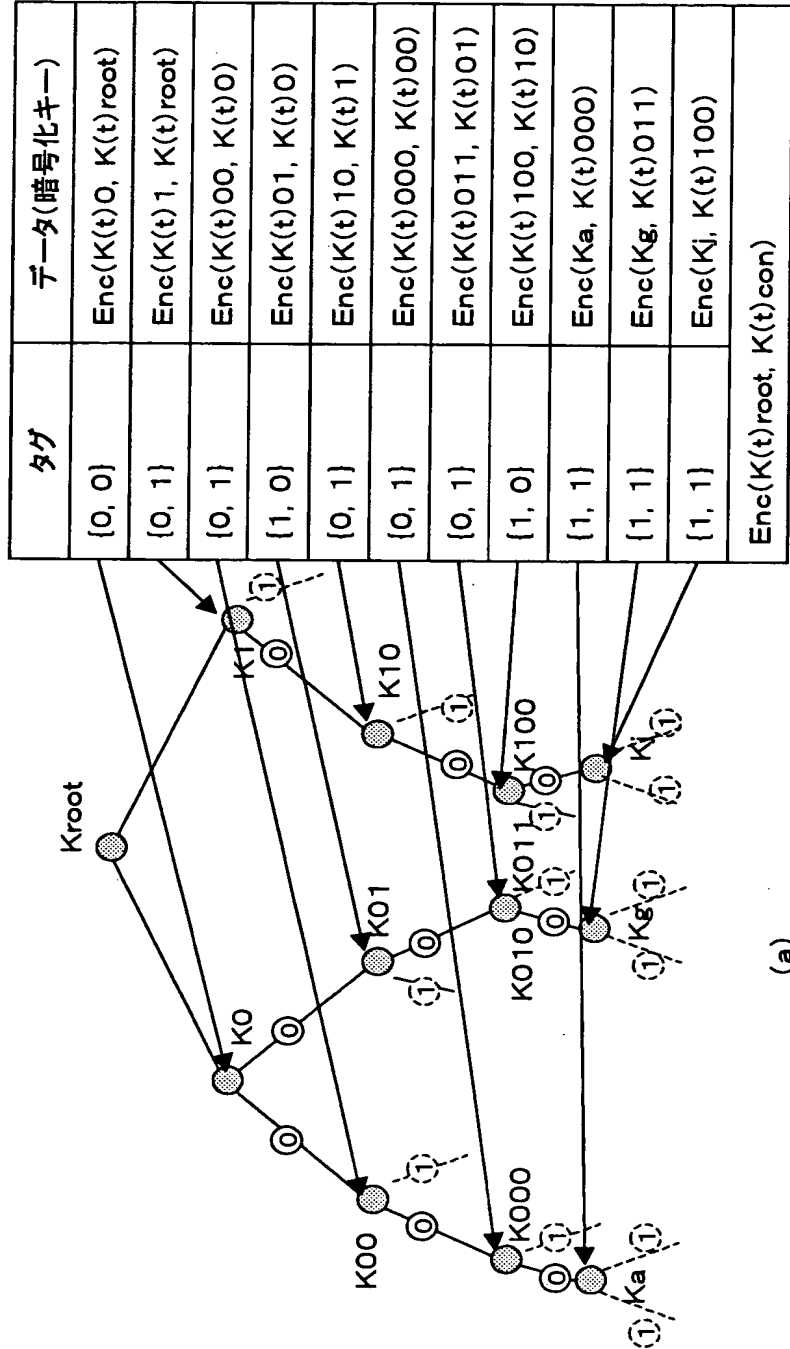
(a)



(b)

【図 1 3】

有効化キーブロック(EKB: Enabling Key Block)を用いた
デバイスKa, Kg, Kjへのバージョンtのコンテンツキー送付処理

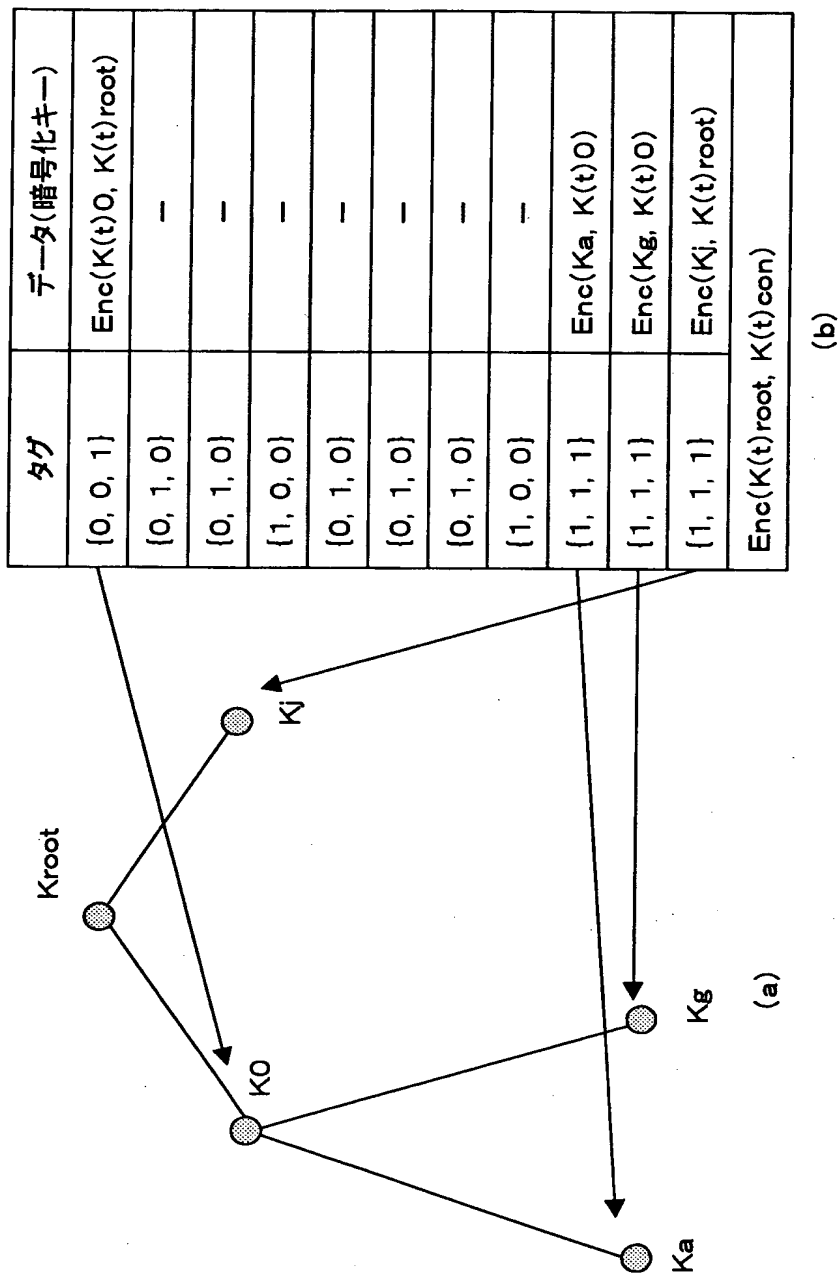


(a)

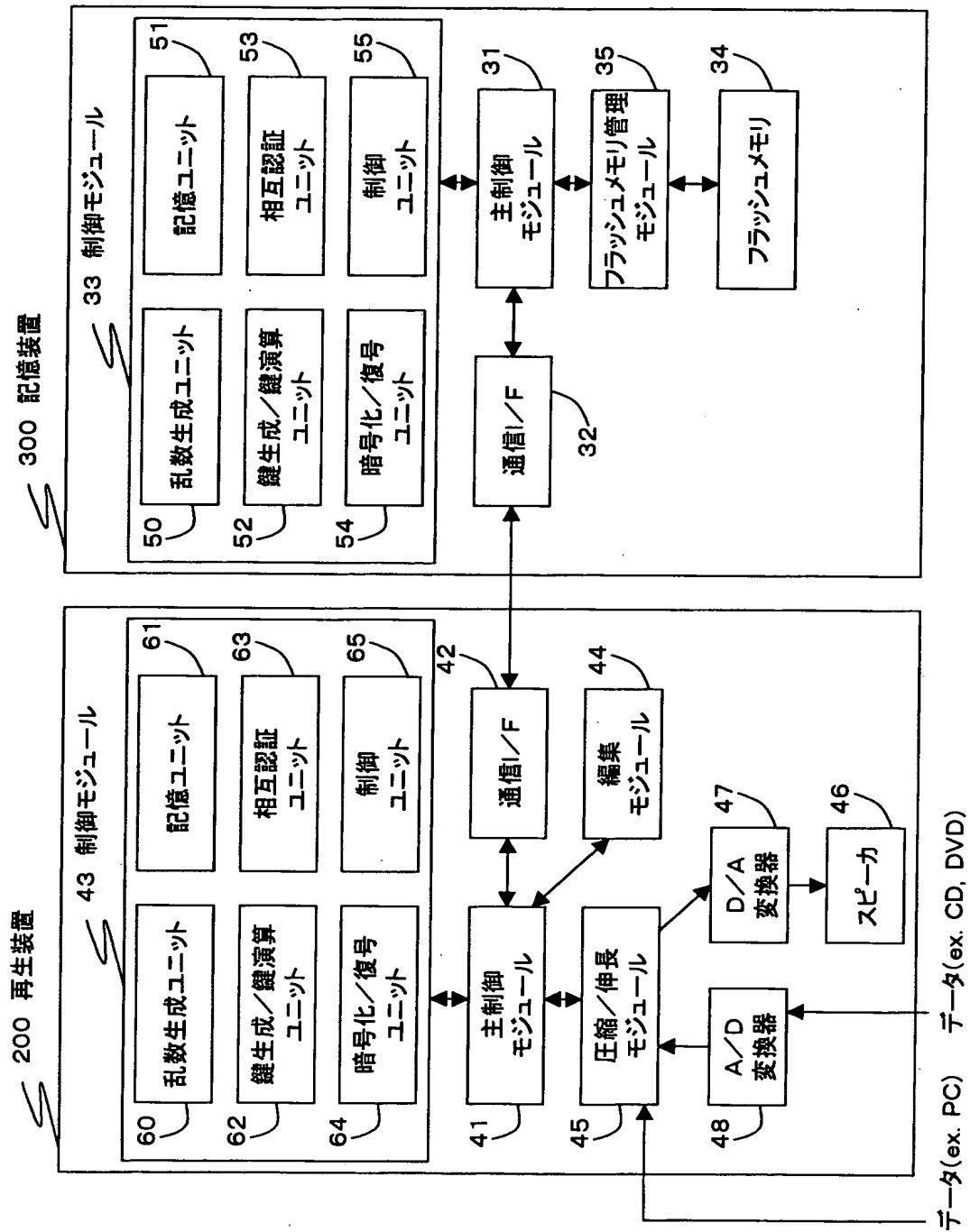
(b)

【図 1 4】

簡略化した有効化キーブロック(EKB: Enabling Key Block)を用いた
デバイスKa, Kg, Kjへのバージョンtのコンテンツキー送付処理



【図15】

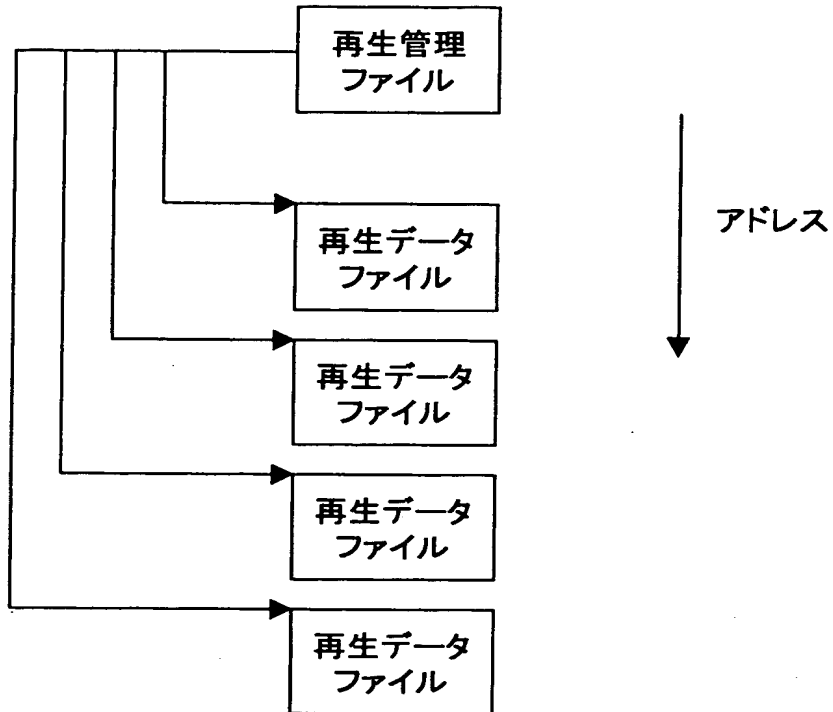


【図 1 6】

記憶装置の記憶ユニットに格納されるデータ

認証鍵データ	IK0
	IK1
	IK2
	IK3
	:
	:
	IK30
	IK31
装置識別データ	ID0
記憶用鍵データ	Kstr

【図 1 7】

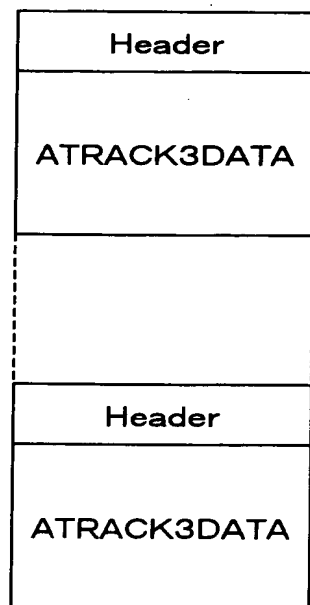
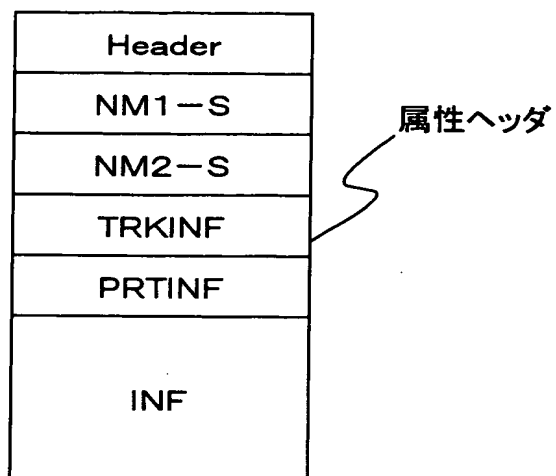


【図 1 8】

再生管理ファイル

Header
NM1-S
NM2-S
TRKTBL
INF-S

【図 1 9】



【図 20】

ATRAC3データファイル

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	BLKID-HD0			Reserved		Mcode		Reservrd				BLOCK SERIAL				
0x0010	N1C+L		N2C+L		INFSIZE		T-PRT		T-SU			INX		XT		
0x0020	NM1-S(256)															
0x0120	NM2-S(512)															
0x0310																
0x0320	Reserved(3)		EKI	EKB version				E(Kstr, Kcon)								
0x0330	E(KEKn, Kcon)							C_MAC[n]								
0x0340	Reserved(8)							INF_seq#			A	LT		FNo		
0x0350	MG(D)SERIAL-nnn(Upper)							MG(D)SERIAL-nnn(Lower)								
0x0360	CONNUM			YMDhms-S				YMDhms-E				MT	CT	CC		CC
0x0370	PRTSIZE			PRTKEY								Reserved(8)				
0x0380				CONNUM0				PRTSIZE(0x0388)			PRTKEY					
0x0390				Reserved(8)							CONNUM0					
	INF(0x0400)															
0x3FFF	BLKID-HD0			Reserved		Mcode		Reservrd				BLOCK SERIAL				
0x4000	BLKID-A3D			Reserved		Mcode		CONNUM0				BLOCK SERIAL				
0x4010	BLOCKSEED							INITIALIZATION VECTOR								
0x4020	SU-000(Nbyte=384byte)															
0x41A0	SU-001(Nbyte)															
0x4320	SU-002(Nbyte)															
0x04A0	SU-041(Nbyte)															
0x7DA0	Reserved(Nbyte=208byte)															
0x7F20	BLK SEED															
0x7FF0	BLKID-A3D			Reserved		Mcode		CONNUM0				BLOCK SERIAL				

【図 2 1】

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	BLKID—HD0			Reserved		Mcode		Reservrd				BLOCK SERIAL				
0x0010	N1C+L		N2C+L		INFSIZE		T—PRT		T—SU				INX		XT	
0x0020	NM1—S(256)															
0x0120	NM2—S(512)															
0x0310																

【図 2 2】

0x0320	Reserved(3)	EKI	EKB version	E(Kstr, Kcon)							
0x0330	E(KEKn, Kcon)			C_MAC[n]							
0x0340	Reserved(8)			INF_seq#		A	LT	FNo			
0x0350	MG(D)SERIAL-nnn(Upper)			MG(D)SERIAL-nnn(Lower)							
0x0360	CONNUM		YMDhms-S	YMDhms-E		MT	CT	CC	CC		

【図 2 3】

bit7: ATRACK3のモード 0: Dual 1: Joint

bit6, 5, 4: 3bitのNはモードの値

N	モード	時間	転送レート	SU	バイト
7	HQ	47min	176kbps	31SU	512
6		58min	146kbps	38SU	424
5	EX	64min	132kbps	42SU	384
4	SP	81min	105kbps	53SU	304
3		90min	94kbps	59SU	272
2	LP	128min	66kbps	84SU	192
1	mono	181min	47kbps	119SU	136
0	mono	258min	33kbps	169SU	96

bit3: Reserved

bit2: データ区分 0: オーディオ 1: その他

bit1: 再生SKIP 0: 通常再生 1: SKIP

bit0: エンファシス 0: OFF 1: ON(50/15 μ S)

【図 2 4】

bit7: コピー許可 0: コピー禁止 1: コピー可

bit6: 世代 0: オリジナル 1: 第1世代以上

HCMS bit5-4: 高速デジタルコピーに関するコピー制御

00: コピー禁止 01: コピー第1世代 10: コピー可
コピー第1世代のコピーした子供はコピー禁止とする

bit3-2: MagicGate認証レベル

00: Level10(Non-MG) 01: Level1

02: Level2 11: Reserved

Level10以外はデバインド、コンバインできません

bit1, 0: Reserved

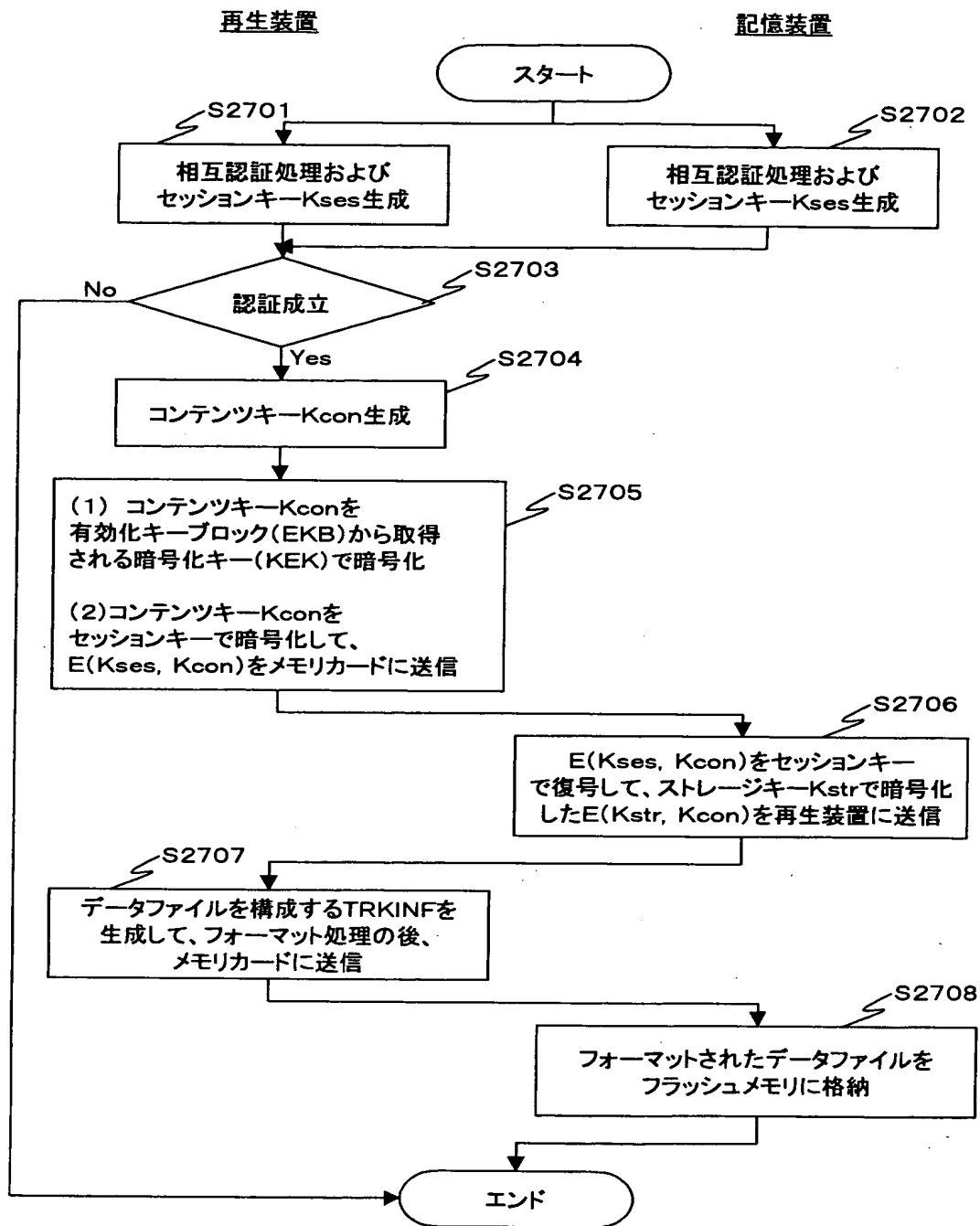
【図 2 5】

0x0370	PRTSIZE	PRTKEY		Reserved(8)
0x0380		CONNUM0	PRTSIZE(0x0388)	PRTKEY
0x0390		Reserved(8)		CONNUM0

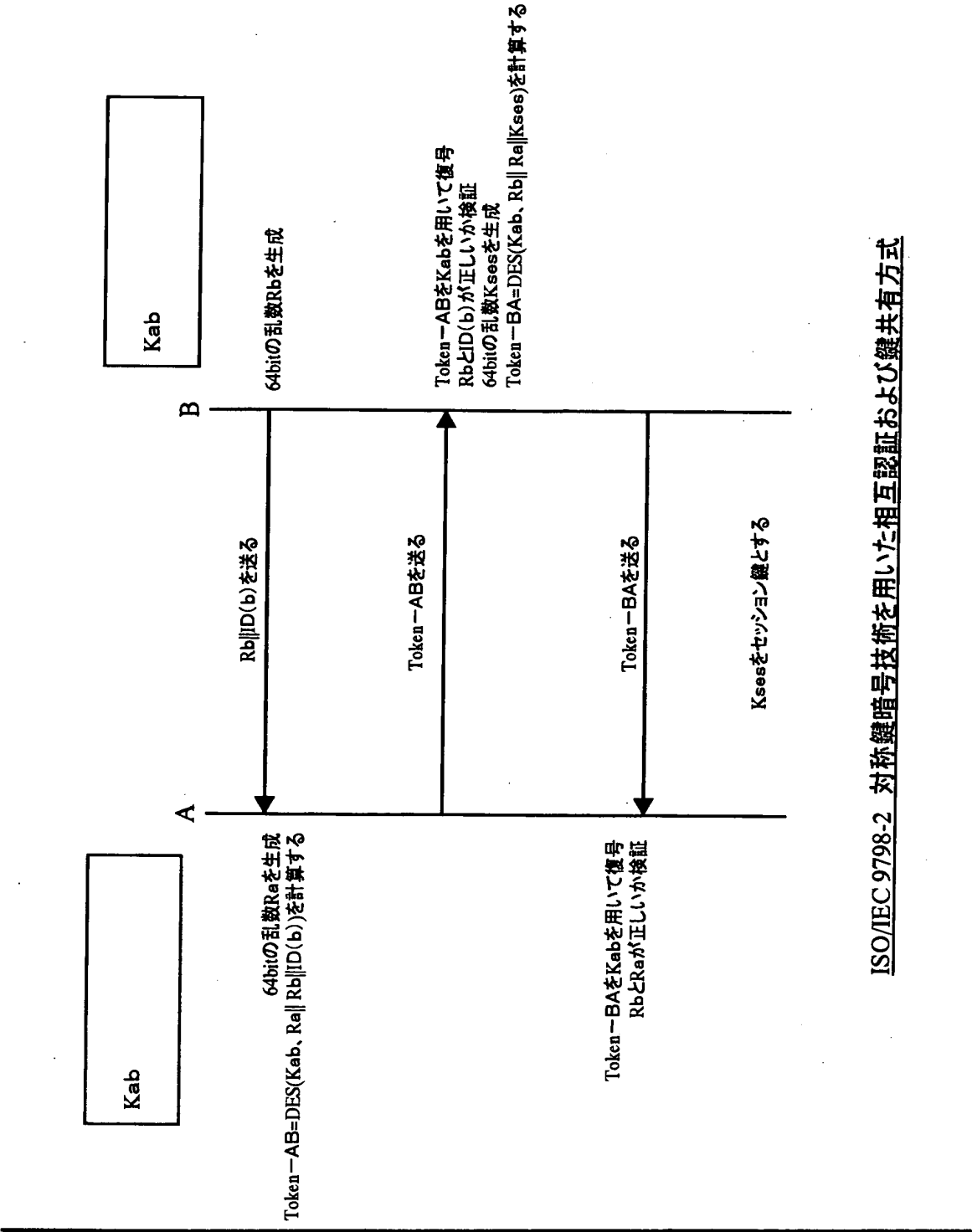
【図 2 6】

0x4000	BLKID—A3D	Reserved	Mcode	CONNUM0	BLOCK SERIAL
0x4010	BLOCKSEED			INITIALIZATION VECTOR	
0x4020	SU—000(Nbyte=384byte)				

【図 2 7】

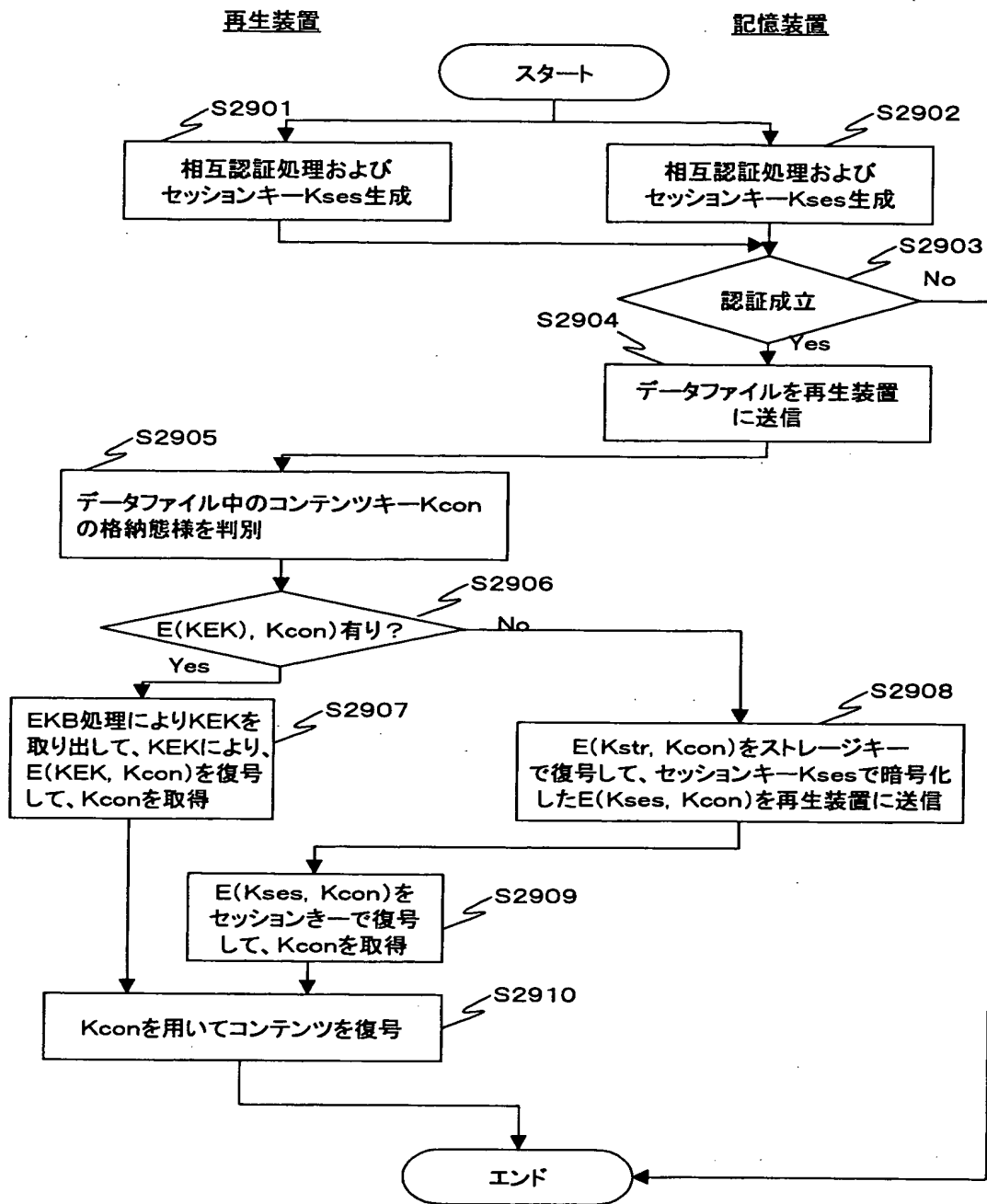


【図 2 8】



ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図 2 9】

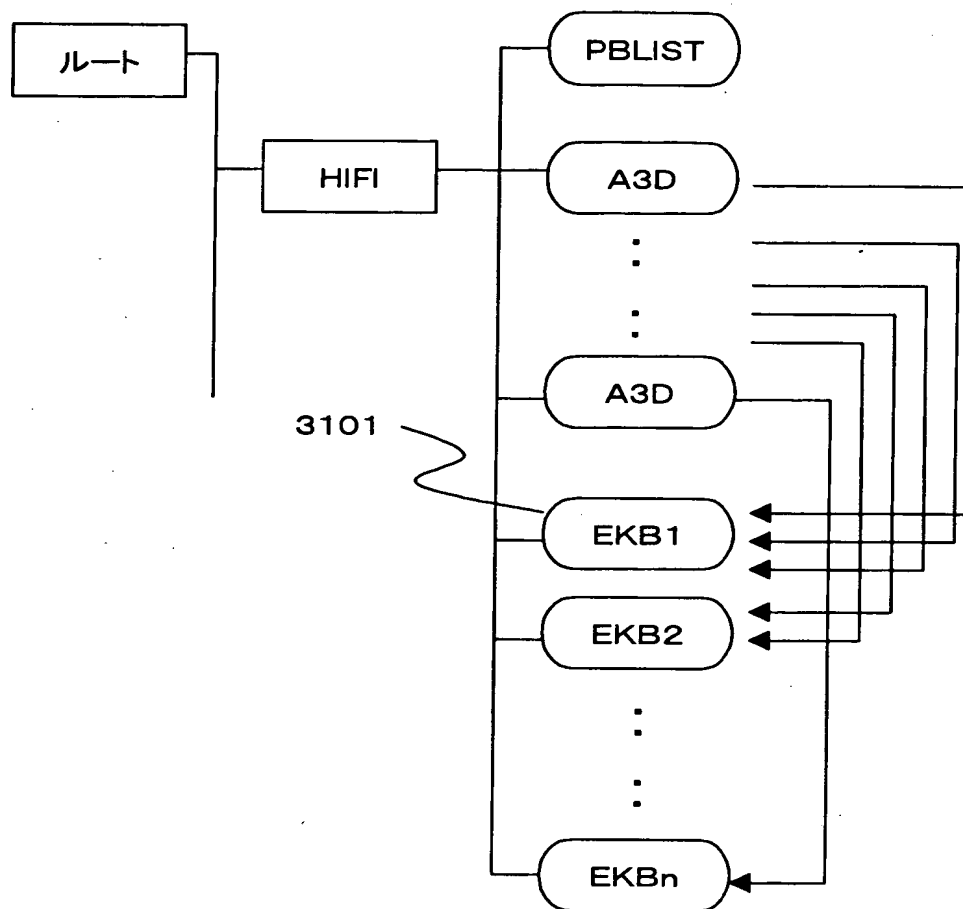


【図 3 0】

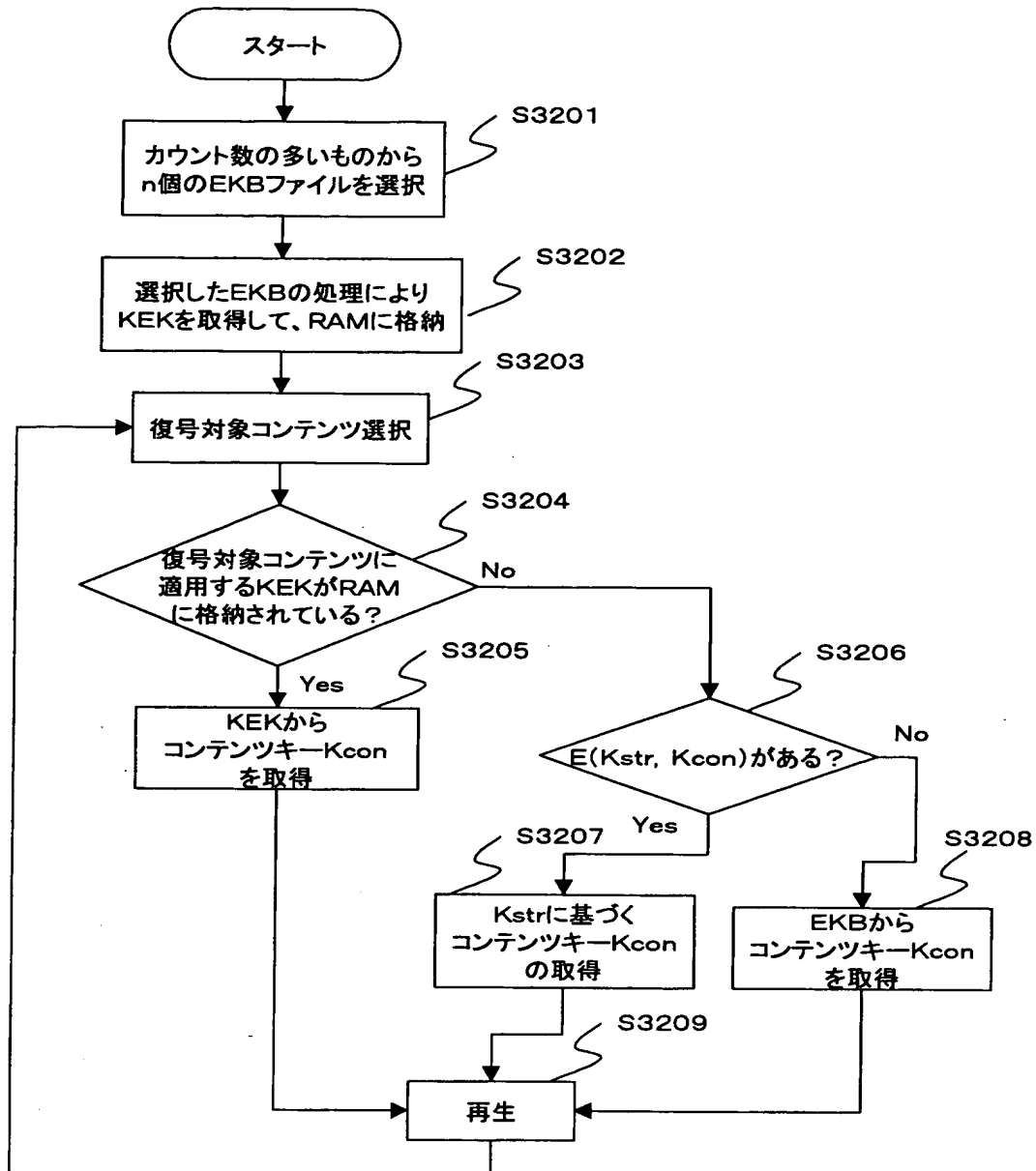
配信鍵許可情報ファイル

0x0000	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0010	BLKID—EKB		Reserved		Mcode		Reserved(3)		LKf		Link Count					
0x0020	Reserved(8)						Reserved(8)									
0x0030	Version		EA		Reserved		KEK1									
0x0040	KEK2						E(Version)									
0x0050	Size of tag part		Size of key part		Size of Sign part											
	Tag part ([X, 0, 0], [X, 1, 1].....)															
	Fill to 64bit alignment															
	Key part															
	Signature															

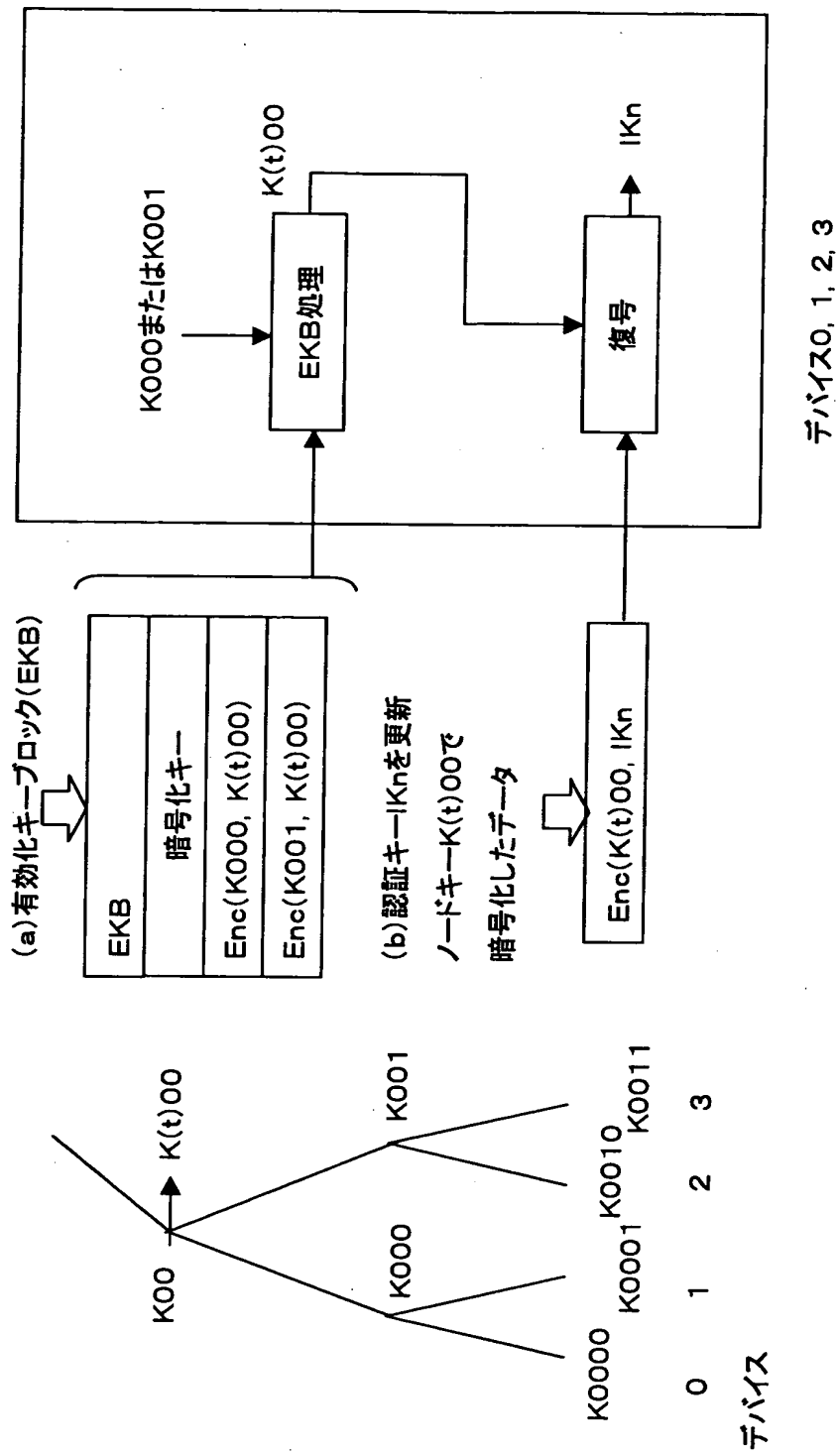
【図 3 1】



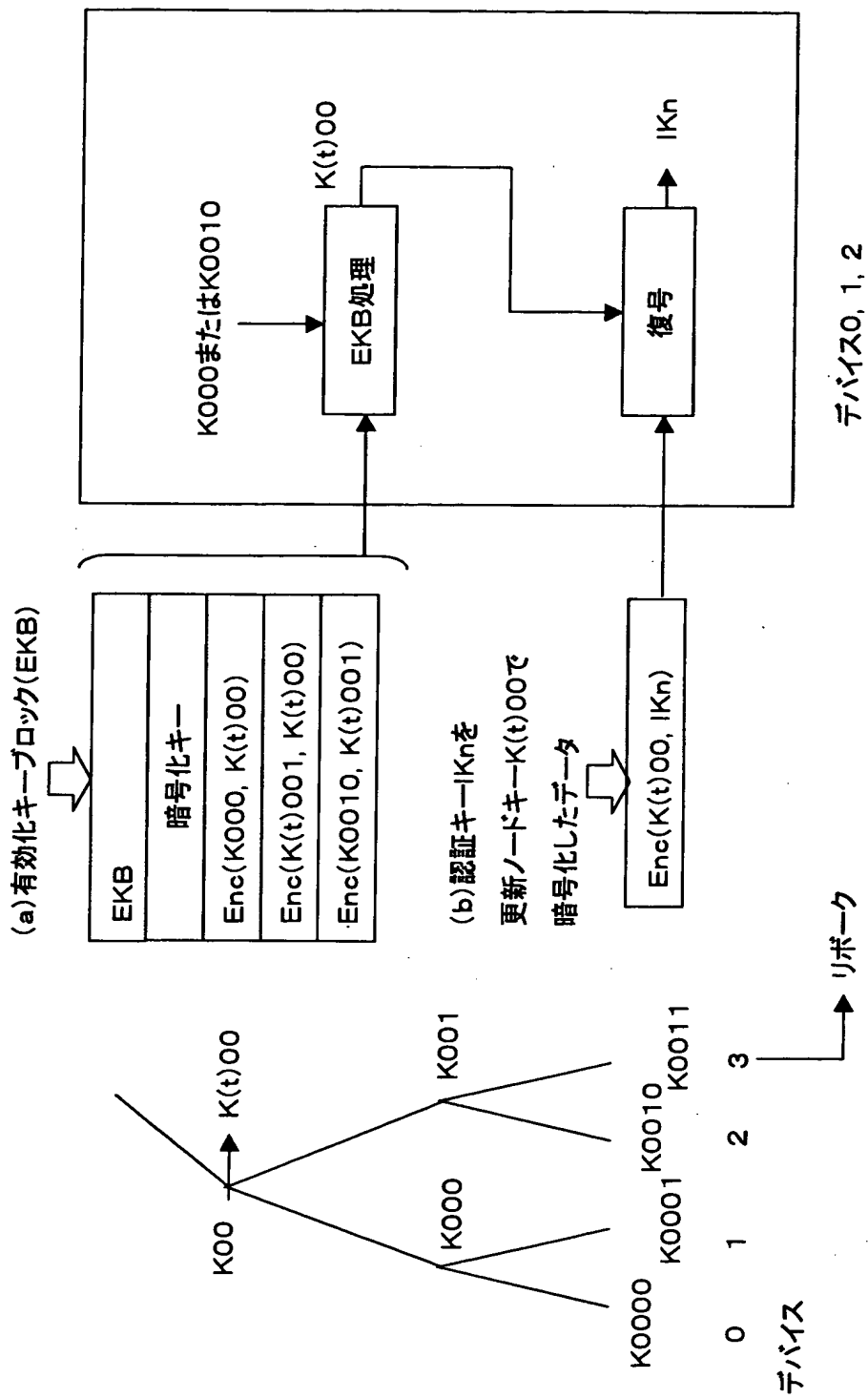
【図 3 2】



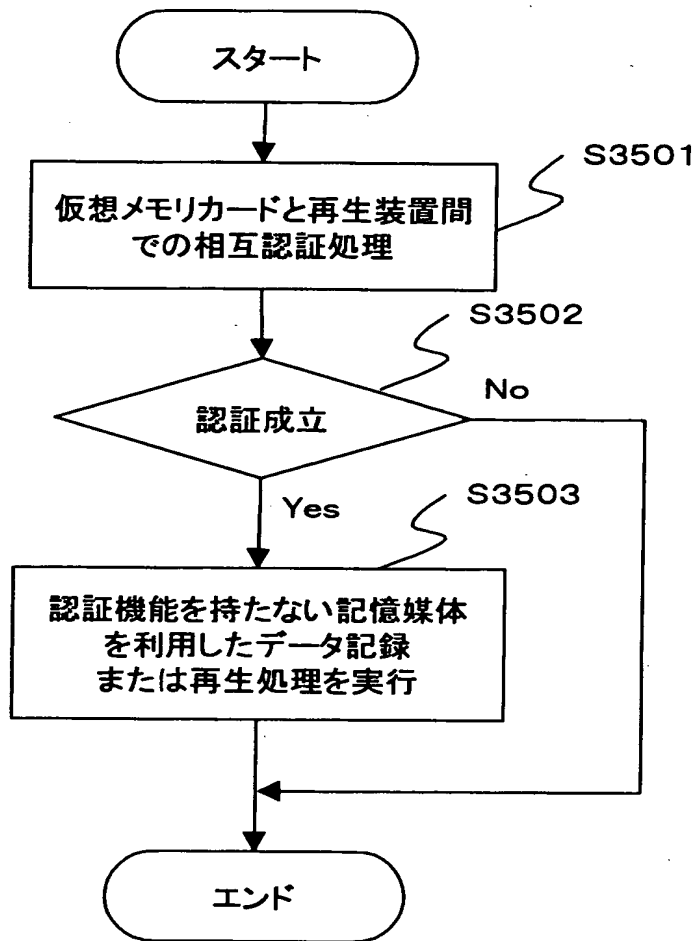
【図 33】



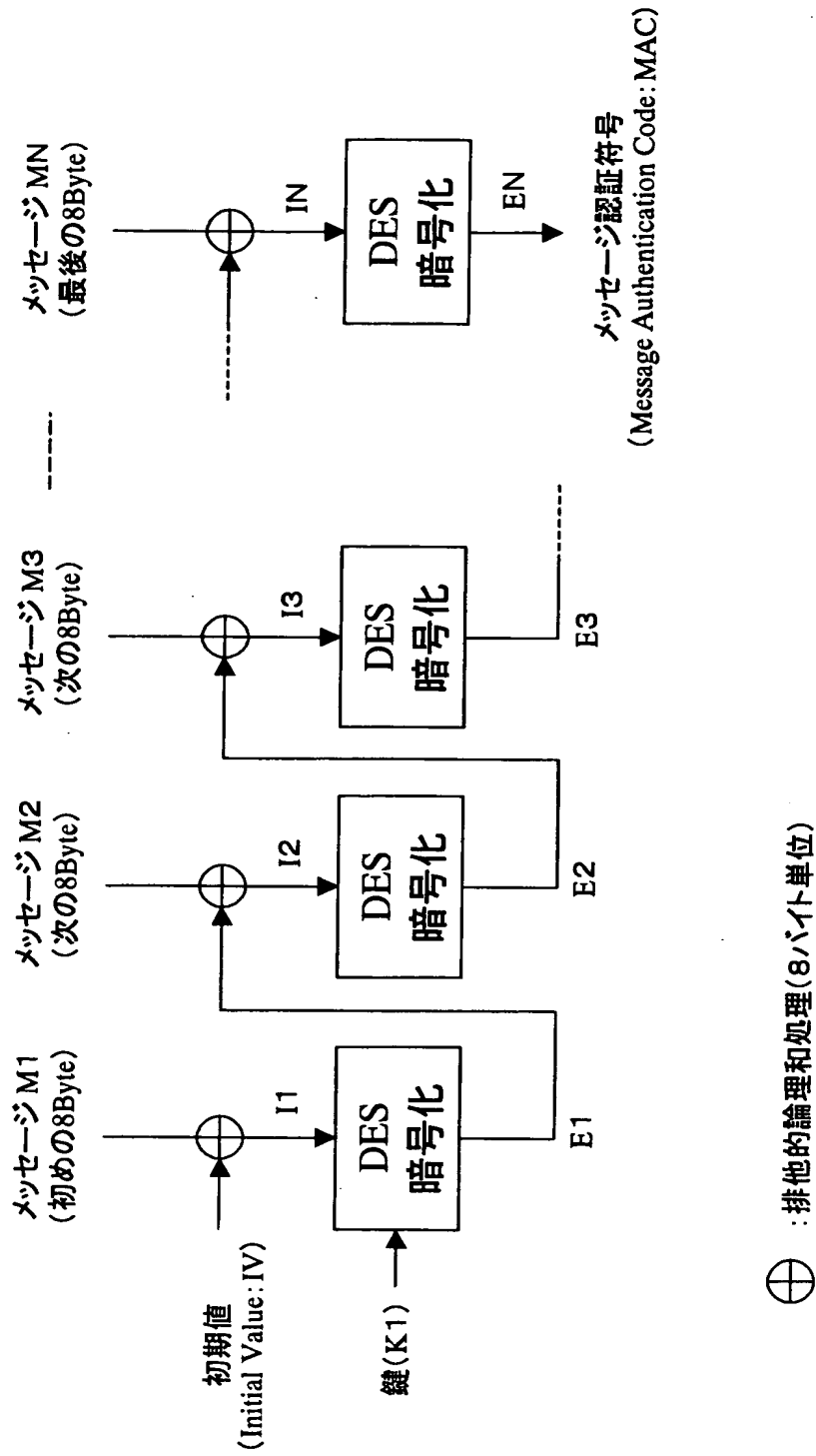
【図 34】



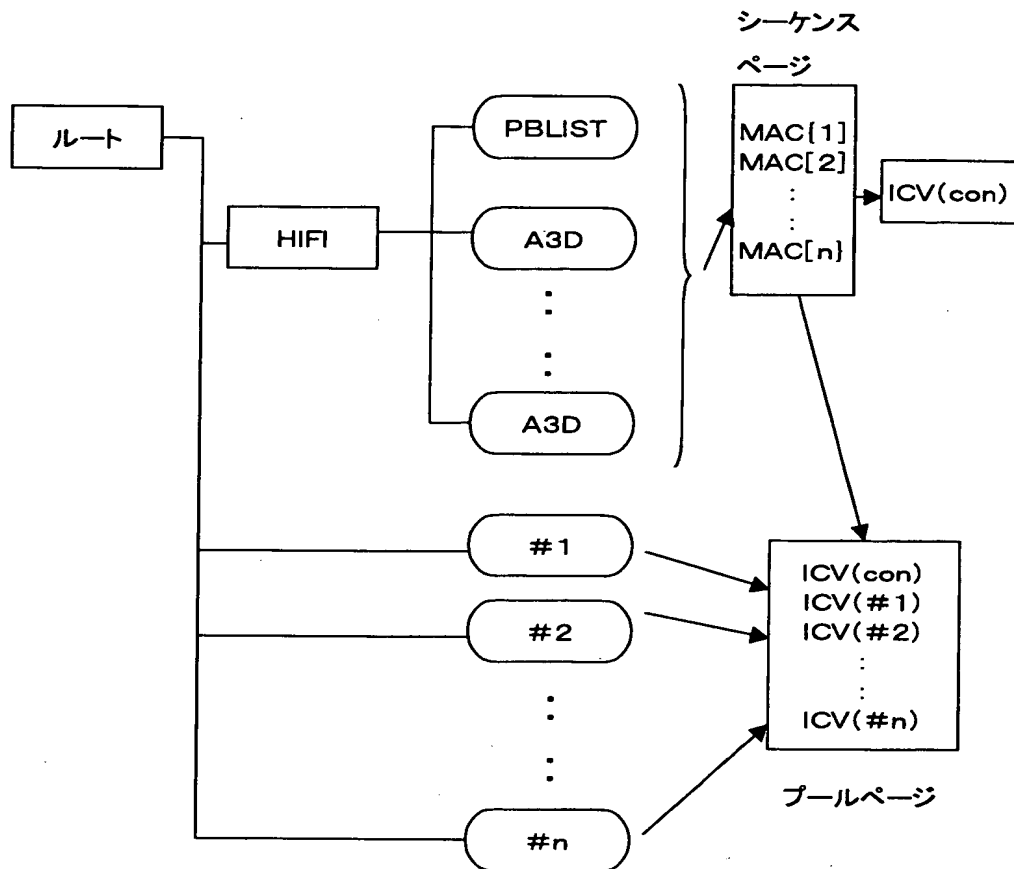
【図 35】



【図 36】



【図 3 7】



【図 3 8】

シーケンスページフォーマット

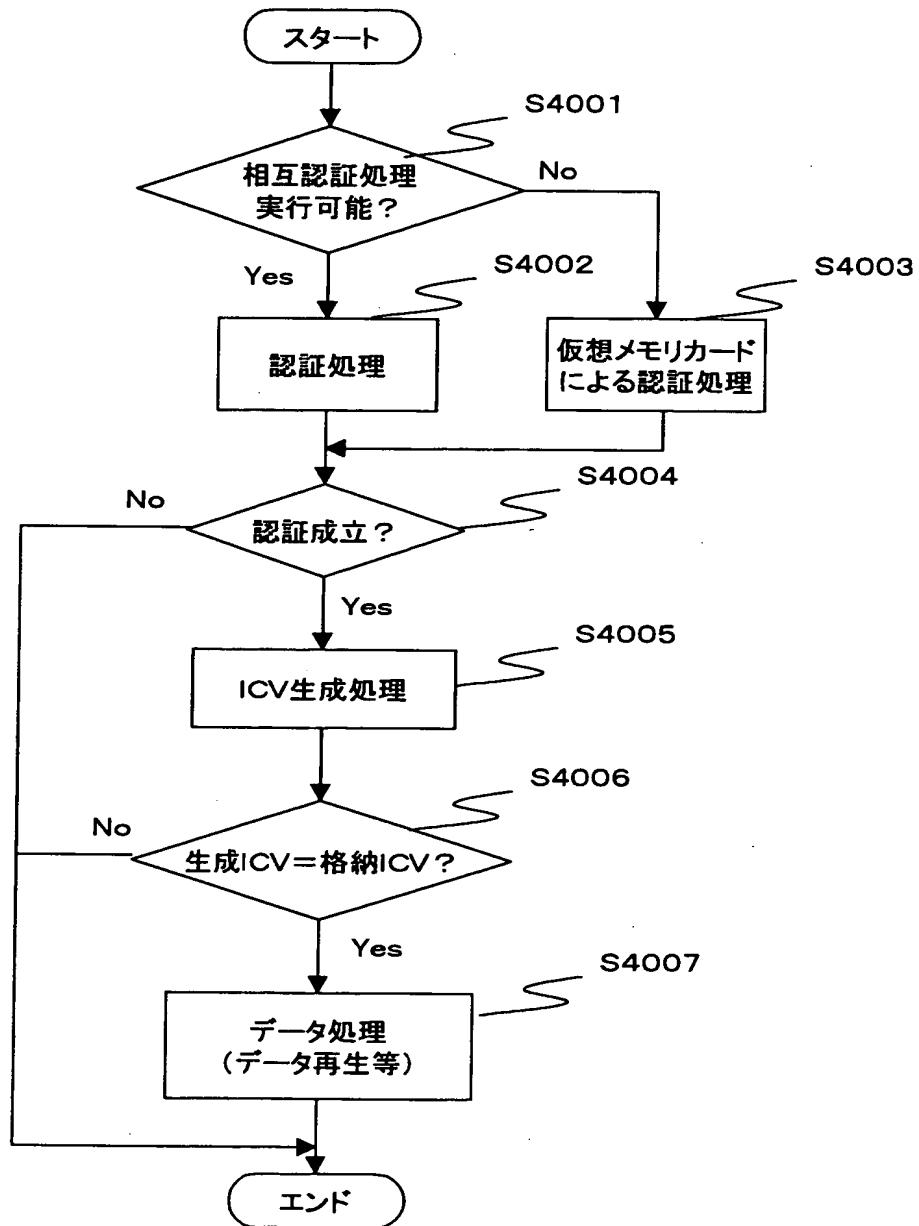
0x0000	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	E(Kstr, Kcon)								Reserved							
0x0010	ID(Upper)								IO(Lower)							
0x0020	C_MAC[0] (PUBLIST)								C_MAC[1]							
0x0030	C_MAC[2]								C_MAC[3]							
0x0FF0	:															
									:							
									:							
	C_MAC[nnn]								Reserved				Revision			

【図 3 9】

ブールページフォーマット

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	#0_revision			#0_EKB version			#0_E(KEK, Kicv)									
0x0010	#0_E(KEK, Kicv)			ICV0												
0x0020	#1_revision			#1_EKB version			#1_E(KEK, Kicv)									
0x0030	#1_E(KEK, Kicv)			ICV1												
	.															
	.															
	.															
	.															
	.															
	.															
0x01E0	#15_revision			#15_EKB version			#15_E(KEK, Kicv)									
0x01F0	#15_E(KEK, Kicv)			ICV15												

【図 4 0】



【書類名】 要約書

【要約】

【課題】 コンテンツの利用を行なうデータ処理装置におけるコンテンツ改竄チェックの効率化を実現した構成を提供する。

【解決手段】 記憶装置に格納されるコンテンツの検証値を生成してコンテンツに対応付けて格納し、コンテンツ改竄の有無を前記検証値により実行する構成において、検証値をコンテンツのカテゴリ毎に生成して格納する。カテゴリは、コンテンツの種類、あるいは、コンテンツの暗号処理鍵として設定されるコンテンツキー K c o n を暗号化して提供する有効化キーブロック (E K B) の管理エンティティ等に基づいて設定することにより、例えば有効化キーブロック (E K B) の管理エンティティ別に、コンテンツデータの検証処理を独立して実行可能となり、効率的な処理が可能となる。

【選択図】 図 3 7

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 2 1 8 5]

1. 変更年月日 1 9 9 0 年 8 月 3 0 日

[変更理由] 新規登録

住 所 東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名 ソニー株式会社